Amazon ECR

Guía del usuario

Versión de API 2015-09-21

Amazon ECR: Guía del usuario

Table of Contents

¿Qué es Amazon EC2 Container Registry?

Amazon EC2 Container Registry (Amazon ECR) es un servicio de registro de imágenes de contenedor administrado por AWS seguro, escalable y fiable. Amazon ECR admite repositorios de imágenes de contenedor privados con permisos basados en recursos que utilizan AWS IAM. Esto es así para que los usuarios especificados o las instancias Amazon EC2 puedan acceder a los repositorios e imágenes de contenedor. Puede utilizar la CLI que prefiera para insertar, extraer y administrar imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI.

> Note
>
> Amazon ECR también admite repositorios de imágenes de contenedores públicos. Para obtener más información, consulte ¿Qué es Amazon ECRPúblico? en la Guía del usuario público de Amazon ECR.

El equipo de servicios de contenedores de AWS mantiene una hoja de ruta pública en GitHub. Contiene información sobre en lo que están trabajando los equipos y permite a todos los clientes de AWS ofrecer comentarios directos. Para obtener más información, consulte Guía de contenedores de AWS.

Componentes de Amazon ECR

Amazon ECR contiene los siguientes componentes:

Registry (Registro)

Cada cuenta de AWS recibe un registro de Amazon ECR. Puede crear repositorios de imágenes en su registro y guardar imágenes en ellos. Para obtener más información, consulte Registros privados deAmazon ECR (p. 14).

Token de autorización

El cliente debe autenticarse en los registros de Amazon ECR como usuario de AWS antes de insertar y extraer imágenes. Para obtener más información, consulte Autenticación de registros privados (p. 14).

Repositorio

El repositorio de imágenes de Amazon ECR contiene imágenes de Docker, imágenes de Open Container Initiative (OCI) y artefactos compatibles con OCI. Para obtener más información, consulte Repositorios privados deAmazon ECR (p. 25).

Política sobre repositorios

Puede controlar el acceso a los repositorios y a las imágenes que contienen mediante políticas. Para obtener más información, consulte Políticas de repositorio (p. 29).

Imagen

Puede insertar y extraer imágenes de contenedor en los repositorios y utilizarlas localmente en su sistema de desarrollo o en definiciones de tareas de Amazon ECS y especificaciones del pod de Amazon EKS. Para obtener más información, consulte Uso de imágenes de Amazon ECR con Amazon ECS (p. 65) y Uso de imágenes de Amazon ECR con Amazon EKS (p. 66).

Características de Amazon ECR

Amazon ECR ofrece las siguientes características:

- Las políticas de ciclo de vida ayudan a administrar el ciclo de vida de las imágenes en los repositorios. Defina reglas que den lugar a la limpieza de imágenes no utilizadas. Puede probar las reglas antes de aplicarlas al repositorio. Para obtener más información, consulte Políticas de ciclo de vida (p. 47).
- El escaneo de imágenes ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Cada repositorio se puede configurar para escaneo al insertar. De este modo, se garantiza que se analice cada nueva imagen insertada en el repositorio. A continuación, puede recuperar los resultados del escaneo de imágenes. Para obtener más información, consulte Escaneo de imágenes (p. 59).
- La replicación entre regiones y cuentas facilita tener sus imágenes donde las necesite. Esto se configura como una opción del registro y es por región. Para obtener más información, consulte Configuración de replicación (p. 17).

Primeros pasos con Amazon ECR

Para utilizar Amazon ECR debe realizar los pasos necesarios para instalar la AWS Command Line Interface y Docker. Para obtener más información, consulte Setting up with Amazon ECR (p. 3) y Introducción a Amazon ECR utilizando la AWS CLI (p. 8).

Precios de las Amazon ECR

Con Amazon ECR, solo paga por la cantidad de datos que almacena en sus repositorios y por la transferencia de datos desde sus inserciones y extracciones de imágenes. Para obtener más información, consulte Precios de Amazon ECR.

Setting up with Amazon ECR

If you've signed up for AWS and have been using Amazon Elastic Container Service (Amazon ECS) or Amazon Elastic Kubernetes Service (Amazon EKS), you are close to being able to use Amazon ECR. The setup process for these two services is similar, as Amazon ECR is an extension to these services. To use the AWS CLI with Amazon ECR, you must use a version of the AWS CLI that supports the latest Amazon ECR features. If you do not see support for an Amazon ECR feature in the AWS CLI, you should upgrade to the latest version. For more information, see http://aws.amazon.com/cli/.

Complete the following tasks to get set up to push a container image to Amazon ECR for the first time. If you have already completed any of these steps, you may skip them and move on to the next step.

Sign up for AWS

When you sign up for AWS, your AWS account is automatically signed up for all services, including Amazon ECR. You are charged only for the services that you use.

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Note your AWS account number, because you'll need it for the next task.

Create an IAM user

Services in AWS, such as Amazon ECR, require that you provide credentials when you access them, so that the service can determine whether you have permission to access its resources. The console requires your password. You can create access keys for your AWS account to access the command line interface or API. However, we don't recommend that you access AWS using the credentials for your AWS account; we recommend that you use AWS Identity and Access Management (IAM) instead. Create an IAM user, and then add the user to an IAM group with administrative permissions or grant this user administrative permissions. You can then access AWS using a special URL and the credentials for the IAM user.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console.

To create an administrator user for yourself and add the user to an administrators group (console)

1. Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.

> **Note**
>
> We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.

2. In the navigation pane, choose Users and then choose Add user.
3. For User name, enter **`Administrator`**.
4. Select the check box next to AWS Management Console access. Then select Custom password, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.
6. Choose Next: Permissions.
7. Under Set permissions, choose Add user to group.
8. Choose Create group.
9. In the Create group dialog box, for Group name enter **`Administrators`**.
10. Choose Filter policies, and then select AWS managed -job function to filter the table contents.
11. In the policy list, select the check box for AdministratorAccess. Then choose Create group.

    > **Note**
    >
    > You must activate IAM user and role access to Billing before you can use the `AdministratorAccess` permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in step 1 of the tutorial about delegating access to the billing console.

12. Back in the list of groups, select the check box for your new group. Choose Refresh if necessary to see the group in the list.
13. Choose Next: Tags.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see Tagging IAM entities in the IAM User Guide.
15. Choose Next: Review to see the list of group memberships to be added to the new user. When you are ready to proceed, choose Create user.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see Access management and Example policies.

To sign in as this new IAM user, sign out of the AWS console, then use the following URL, where your_aws_account_id is your AWS account number without the hyphens (for example, if your AWS account number is `1234-5678-9012`, your AWS account ID is `123456789012`):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Enter the IAM user name and password that you just created. When you're signed in, the navigation bar displays "your_user_name @ your_aws_account_id".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, choose Customize and enter an Account Alias, such as your company name. For more information, see Your AWS Account ID and Its Alias in the IAM User Guide.

To sign in after you create an account alias, use the following URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

To verify the sign-in link for IAM users for your account, open the IAM console and check under IAM users sign-in link on the dashboard.

For more information about IAM, see the AWS Identity and Access Management User Guide.

Introducción a Amazon ECR utilizando la Consola de administración de AWS

Empiece a trabajar con Amazon ECR creando un repositorio en la consola de Amazon ECR. La consola de Amazon ECR le sirve de guía para empezar a crear su primer repositorio.

Antes de comenzar, asegúrese de que ha realizado los pasos que se detallan en Setting up with Amazon ECR (p. 3).

Para crear un repositorio de imágenes

Un repositorio es donde almacena las imágenes de Docker u Open Container Initiative (OCI) en Amazon ECR. Cada vez que inserta o extrae una imagen de Amazon ECR, debe especificar la ubicación del registro y el repositorio que indica adónde se va a enviar la imagen o de dónde se la va a extraer.

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. Elija Get Started.
3. En Tag mutability (Mutabilidad de etiquetas), seleccione la configuración de mutabiilidad de etiquetas del repositorio. Los repositorios configurados con etiquetas inmutables impedirán que se sobrescriban las etiquetas de imagen. Para obtener más información, consulte Mutabilidad de etiquetas de imágenes (p. 58).
4. En Scan on push (Escanear al insertar), elija la configuración de escaneo de imágenes para el repositorio. Los repositorios configurados para escanear al insertar comenzarán un escaneo de imagen cada vez que se inserte una imagen; de lo contrario, los escaneos de imágenes deben iniciarse manualmente. Para obtener más información, consulte Escaneo de imágenes (p. 59).
5. Elija Create repository (Crear repositorio).

Creación, etiquetado y envío de una imagen de Docker

En esta sección del asistente, puede utilizar la CLI de Docker para etiquetar una imagen local existente (que ha creado a partir de un Dockerfile o extraído de otro registro, como Docker Hub) y, a continuación, enviar la imagen etiquetada a su su registro de Amazon ECR. Para obtener instrucciones más detalladas sobre el uso de la CLI de Docker, consulte Introducción a Amazon ECR utilizando la AWS CLI (p. 8).

1. Seleccione el repositorio que ha creado y elija View push commands (Ver comandos de inserción) para ver los pasos para insertar una imagen en su nuevo repositorio.
2. Recupere el comandodocker login que puede utilizar para autenticar su cliente Docker en el registro pegando el comando aws ecr get-login desde la consola en una ventana de terminal.

   Note

   El comando get-login está disponible en la AWS CLI; a partir de 1.9.15; no obstante, le recomendamos la versión 1.11.91 o posterior para las versiones recientes de Docker (17.06 o posterior). Puede comprobar la versión de la AWS CLI con el comando aws --version. Si utiliza Docker versión 17.06 o posterior, incluya la opción `--no-include-email` después de `get-login`. Si recibe un error `Unknown options: --no-include-email`, instale la última versión de AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

3. Ejecute el comando docker login que se devolvió en el paso anterior. Este comando proporciona un token de autorización que es válido durante 12 horas.

   Important

   Si ejecuta este comando docker login, otros usuarios del sistema podrán ver la cadena del comando en una pantalla de lista de procesos (ps -e). Como el comando docker login contiene las credenciales de autenticación, existe el riesgo de que otros usuarios de su sistema puedan verlas y usarlas para obtener acceso de recepción y envío a sus repositorios. Pueden usar las credenciales para obtener acceso de recepción y envío a sus repositorios. Si no se encuentra en un sistema seguro, deberá considerar este riesgo e iniciar sesión de forma interactiva omitiendo la opción `-p` *`password`* y después introducir la contraseña cuando se le solicite.
4. (Opcional) Si tiene un Dockerfile para la imagen que va a insertar, compile la imagen y etiquétela para su nuevo repositorio: pegando el comando docker build de la consola en una ventana de terminal. Asegúrese de que se encuentra en el mismo directorio que su Dockerfile.
5. Etiquete la imagen para su nuevo repositorio y registro de ECR pegando el comando docker tag desde la consola en una ventana de terminal. El comando de la consola presupone que la imagen se creó desde un Dockerfile en el paso anterior; si no creó la imagen desde un Dockerfile, sustituya la primera instancia de *`repository`*`:latest` por el ID o el nombre de imagen de la imagen local que desea insertar.
6. Inserte la imagen recién etiquetada en su repositorio de ECR pegando el comando docker push en una ventana de terminal.
7. Elija Close (Cerrar).

Introducción a Amazon ECR utilizando la AWS CLI

Los siguientes pasos le guiarán por los pasos necesarios para insertar una imagen de contenedor a Amazon ECR por primera vez utilizando la CLI de Docker y la AWS CLI.

Para obtener más información sobre otras herramientas de administración de recursos de AWS, incluidos los distintos conjuntos de herramientas de IDE, el SDK de AWS y las herramientas de línea de comandos de Windows PowerShell, consulte http://aws.amazon.com/tools/.

Requisitos previos

Antes de comenzar, asegúrese de que ha realizado los pasos que se detallan en Setting up with Amazon ECR (p. 3).

Si aún no dispone de la versión más reciente de la AWS CLI y Docker instaladas y listas para usarse, siga los pasos siguientes para instalar estas dos herramientas.

Instalar la AWS CLI

Puede utilizar las herramientas de línea de comandos de AWS para emitir comandos en la línea de comando de su sistema con el fin de llevar a cabo tareas de Amazon ECR y de AWS. Esto puede ser más rápido y práctico que usar la consola. Las herramientas de línea de comandos también son útiles para crear scripts que realicen tareas de AWS.

Para usar la AWS CLI con Amazon ECR, instale la última versión de la AWS CLI (la funcionalidad de Amazon ECR está disponible en la AWS CLI a partir de la versión 1.9.15). Puede comprobar la versión de la AWS CLI con el comando aws --version. Para obtener más información sobre la instalación de la AWS CLI o cómo realizar la actualización a la versión más reciente, consulte Instalación de la CLI versión 2 de AWS en la AWS Command Line Interface Guía del usuario.

Instalar Docker

Docker está disponible en muchos sistemas operativos diferentes, incluidas las distribuciones de Linux más modernas, como Ubuntu, e incluso en Mac OSX y Windows. Para obtener más información sobre cómo instalar Docker en su sistema operativo concreto, consulte la guía de instalación de Docker.

No necesita un sistema de desarrollo local para usar Docker. Si ya utiliza Amazon EC2, puede lanzar una instancia de Amazon Linux 2 e instalar Docker para comenzar.

Si ya tiene Docker instalado, pase a Paso 1: creación de una imagen de Docker (p. 9).

Para instalar Docker en una instancia de Amazon EC2

1. Lance una instancia con la AMI de Amazon Linux 2. Para obtener más información, consulte Lanzar una instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.
2. Conéctese a la instancia. Para obtener más información, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Actualice la caché de paquetes y los paquetes instalados en la instancia.

```
sudo yum update -y
```

4. Instale el paquete de Community Edition de Docker más reciente.

```
sudo amazon-linux-extras install docker
```

5. Abra el servicio de Docker.

```
sudo service docker start
```

6. Agregue el `ec2-user` al grupo `docker` para que pueda ejecutar comandos de Docker sin usar `sudo`.

```
sudo usermod -a -G docker ec2-user
```

7. Cierre sesión y vuelva a iniciarla para actualizar los nuevos permisos de grupo de `docker`. Para ello, cierre la ventana de su terminal de SSH actual y vuelva a conectarse a la instancia en una ventana nueva. De esta forma, la nueva sesión de SSH tendrá los permisos de grupo de `docker` adecuados.
8. Compruebe que el `ec2-user` puede ejecutar comandos de Docker sin `sudo`.

```
docker info
```

Note

En algunos casos, es posible que tenga que reiniciar su instancia para que el `ec2-user` tenga los permisos necesarios para acceder al demonio de Docker. Intente reiniciar su instancia si ve el siguiente error:

```
Cannot connect to the Docker daemon. Is the docker daemon running on this host?
```

Paso 1: creación de una imagen de Docker

En esta sección va a crear una imagen Docker de una aplicación web simple y probarla en su sistema local o su instancia de EC2. Luego enviará la imagen a un registro de contenedor (como Amazon ECR o Docker Hub) para poder utilizarla en una definición de tarea de ECS.

Creación de una imagen Docker de una aplicación web simple

1. Cree un archivo denominado `Dockerfile`. Un Dockerfile es un manifiesto que describe la imagen base para su imagen Docker y qué desea instalar y que se ejecute en ella. Para obtener más información acerca de los archivos Docker, consulte Docker Reference.

```
touch Dockerfile
```

2. Editar el `Dockerfile` que acaba de crear y añadir el siguiente contenido.

```
FROM ubuntu:18.04

# Install dependencies
RUN apt-get update && \
 apt-get -y install apache2

# Install apache and write hello world message
RUN echo 'Hello World!' > /var/www/html/index.html
```

```
# Configure apache
RUN echo '. /etc/apache2/envvars' > /root/run_apache.sh && \
 echo 'mkdir -p /var/run/apache2' >> /root/run_apache.sh && \
 echo 'mkdir -p /var/lock/apache2' >> /root/run_apache.sh && \
 echo '/usr/sbin/apache2 -D FOREGROUND' >> /root/run_apache.sh && \
 chmod 755 /root/run_apache.sh

EXPOSE 80

CMD /root/run_apache.sh
```

Este Dockerfile utiliza la imagen Ubuntu 18.04. Las instrucciones `RUN` actualizan las cachés de paquete, instalan algunos paquetes de software para el servidor web y, a continuación, escriben el contenido "Hello World!" en la raíz de documentos del servidor web. El folleto `EXPOSE` expone el puerto 80 en el contenedor y las instrucciones `CMD` inician el servidor web.

3. Cree la imagen Docker desde el Dockerfile.

   Note

   Algunas versiones de Docker pueden requerir la ruta completa a su Dockerfile en el siguiente comando en lugar de la ruta relativa que se muestra a continuación.

```
docker build -t hello-world .
```

4. Ejecute docker images para comprobar que la imagen se haya creado correctamente.

```
docker images --filter reference=hello-world
```

   Salida:

```
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
hello-world         latest              e9ffedc8c286        4 minutes ago       241MB
```

5. Ejecute la nueva imagen. La opción `-p 80:80` asigna el puerto 80 expuesto en el contenedor al puerto 80 del sistema de host. Para obtener más información acerca de docker run, diríjase a la referencia de ejecución de Docker.

```
docker run -t -i -p 80:80 hello-world
```

   Note

   La salida desde el servidor web Apache se muestra en la ventana de la terminal. Puede hacer caso omiso del mensaje "`Could not reliably determine the server's fully qualified domain name`"

6. Abra un navegador y encuentre el servidor que está ejecutando Docker y alojando su contenedor.

   - Si utiliza una instancia de EC2, este es el valor DNS público para el servidor, que es la misma dirección que utiliza para conectarse a la instancia con SSH. Asegúrese de que el grupo de seguridad para la instancia permite el tráfico entrante en el puerto 80.
   - Si ejecuta Docker de forma local, dirija el navegador a http://localhost/.
   - Si utiliza docker-machine en un equipo Windows o Mac, encuentre la dirección IP del VirtualBox VM que aloja Docker con el comando docker-machine ip y sustituya *machine-name* con el nombre de la máquina docker que esté usando.

```
docker-machine ip machine-name
```

Debería ver una página web con la declaración "Hello World!".

7. Detenga el contenedor de Docker escribiendo Ctrl + c.

Paso 2: autenticar en su registro predeterminado

Una vez instalada y configurada la AWS CLI, puede autenticar la CLI de Docker en el registro predeterminado. De este modo, el comando docker puede extraer e insertar imágenes con Amazon ECR. La AWS CLI proporciona un comando get-login-password que simplifica el proceso de autenticación.

Para autenticar Docker en un registro de Amazon ECR con get-login-password, ejecute el comando aws ecr get-login-password. Al pasar el token de autenticación al comando docker login, utilice el valor `AWS` para el nombre de usuario y especifique el URI del registro de Amazon ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

> **Important**
>
> Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

- get-login-password (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- Get-ECRLoginCommand (Herramientas de AWS para Windows PowerShell)

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Paso 3: crear un repositorio

Ahora que ya tiene una imagen para insertar en Amazon ECR, debe crear un repositorio para almacenarla. En este ejemplo, va a crear un repositorio llamado `hello-world` en el que insertará después la imagen `hello-world:latest`. Para crearlo, ejecute este comando:

```
aws ecr create-repository \
    --repository-name hello-world \
    --image-scanning-configuration scanOnPush=true \
    --region us-east-1
```

Paso 4: insertar una imagen en Amazon ECR

Inserte la imagen en el repositorio de Amazon ECR que ha creado en la sección anterior. Las imágenes se insertan mediante la CLI de docker. Para que este procedimiento funcione correctamente, deben cumplirse una serie de requisitos previos:

- La versión instalada es la versión mínima de docker: 1.7.

- El código de autorización de Amazon ECR se ha configurado con docker login.
- Debe existir el repositorio de Amazon ECR y el usuario debe obtener acceso para insertar imágenes en él.

Si se cumplen estos requisitos previos, podrá insertar la imagen en el repositorio recién creado del registro predeterminado de su cuenta.

Para etiquetar e insertar una imagen en Amazon ECR

1. Muestre las imágenes que ha almacenado localmente para identificar la que desea etiquetar e insertar.

```
docker images
```

Salida:

```
REPOSITORY          TAG                 IMAGE ID            CREATED             VIRTUAL
 SIZE
hello-world         latest              e9ffedc8c286        4 minutes ago       241MB
```

2. Etiquete la imagen que desea insertar en el repositorio.

```
docker tag hello-world:latest aws_account_id.dkr.ecr.us-east-1.amazonaws.com/hello-
world:latest
```

3. Inserte la imagen.

```
docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

Salida:

```
The push refers to a repository [aws_account_id.dkr.ecr.us-east-1.amazonaws.com/hello-
world] (len: 1)
e9ae3c220b23: Pushed
a6785352b25c: Pushed
0998bf8fb9e9: Pushed
0a85502c06c9: Pushed
latest: digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636b95aed25f52c89b
 size: 6774
```

Paso 5: extraer una imagen de Amazon ECR

Una vez insertada la imagen en el repositorio de Amazon ECR, puede extraerla de otras ubicaciones. Utilice la CLI de docker. Para que este procedimiento funcione correctamente, deben cumplirse una serie de requisitos previos:

- La versión instalada es la versión mínima de docker: 1.7.
- El código de autorización de Amazon ECR se ha configurado con docker login.
- Debe existir el repositorio de Amazon ECR y el usuario debe tener acceso para extraer imágenes de él.

Si se cumplen estos requisitos previos, podrá extraer la imagen. Para extraer la imagen de ejemplo de Amazon ECR, ejecute este comando:

```
docker pull aws_account_id.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

Salida:

```
latest: Pulling from hello-world
0a85502c06c9: Pull complete
0998bf8fb9e9: Pull complete
a6785352b25c: Pull complete
e9ae3c220b23: Pull complete
Digest: sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636b95aed25f52c89b
Status: Downloaded newer image for aws_account_id.dkr.ecr.us-east-1.amazonaws.com/hello-
world:latest
```

Paso 6: eliminar una imagen

Si decide que ya no necesita o no quiere una imagen de uno de los repositorios, puede eliminarla con el comando batch-delete-image. Para eliminar una imagen, debe especificar el repositorio en el que está y un valor `imageTag` o `imageDigest` para ella. En el ejemplo siguiente eliminaremos una imagen del repositorio `hello-world` con la etiqueta de imagen `latest`.

```
aws ecr batch-delete-image \
      --repository-name hello-world \
      --image-ids imageTag=latest
```

Salida:

```
{
    "failures": [],
    "imageIds": [
        {
            "imageTag": "latest",
            "imageDigest":
 "sha256:215d7e4121b30157d8839e81c4e0912606fca105775bb0636b95aed25f52c89b"
        }
    ]
}
```

Paso 7: eliminar un repositorio

Si decide que ya no necesita o no quiere un repositorio completo de imágenes, puede eliminarlo. De forma predeterminada, no puede eliminar un repositorio que contenga imágenes; no obstante, la marca `--force` le permite hacerlo. Para eliminar un repositorio que contiene imágenes (y todas las imágenes incluidas en él), ejecute este comando.

```
aws ecr delete-repository \
      --repository-name hello-world \
      --force
```

Registros privados deAmazon ECR

Los registros privados de Amazon ECR de alojan sus imágenes de contenedor en una arquitectura escalable y de alta disponibilidad. Puede utilizar su registro privado para administrar repositorios de imágenes privadas compuestos de imágenes y artefactos de Docker y Open Container Initiative (OCI). A cada cuenta de AWS se le suministra un registro de Amazon ECR público y privado predeterminado. Para obtener más información acerca de los registros públicos, consulte Registros públicos en la Guía del usuario público de Amazon EC2 Container Registry.

Conceptos del registro privado

- La dirección URL del registro privado predeterminado es `https://aws_account_id.dkr.ecr.region.amazonaws.com`.
- De forma predeterminada, su cuenta tiene acceso de lectura y escritura en los repositorios de su registro privado. Sin embargo, los usuarios de IAM necesitan permisos para realizar llamadas al Amazon ECR APIs y para insertar o extraer imágenes en o de sus repositorios privados. Amazon ECR proporciona varias políticas administradas para controlar el acceso de los usuarios en diferentes niveles. Para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).
- Debe autenticar su cliente Docker en su registro privado para poder utilizar los comandos docker push y docker pull para insertar y extraer imágenes en y desde los repositorios de ese registro. Para obtener más información, consulte Autenticación de registros privados (p. 14).
- Los repositorios privados se pueden controlar mediante políticas de acceso de usuarios de IAM y políticas de repositorio. Para obtener más información acerca de las políticas de repositorios, consulte Políticas de repositorio (p. 29).
- Las imágenes se pueden replicar en otros repositorios de entre regiones de su propio registro y entre cuentas especificando una configuración de replicación en su configuración de registro. Para obtener más información, consulte Configuración de replicación (p. 17).

Autenticación de registros privados

Puede utilizar la Consola de administración de AWS, la AWS CLI o la AWS SDKs para crear y administrar repositorios. También puede utilizar estos métodos para realizar determinadas acciones con las imágenes, por ejemplo listarlas o eliminarlas. Estos clientes usan métodos de autenticación de AWS estándar. Aunque puede utilizar la API de Amazon ECR para insertar y extraer imágenes, es más probable que utilice la CLI de Docker o una biblioteca de Docker específica del lenguaje.

La CLI de Docker no admite métodos de autenticación de IAM nativos. Se deben tomar pasos adicionales para que Amazon ECR pueda autenticar y autorizar solicitudes de inserción y extracción de Docker.

Los métodos de autenticación del registro que se detallan en las siguientes secciones están disponibles.

Uso del auxiliar de credenciales de laAmazon ECR

Amazon ECR proporciona un ayudante de credenciales de Docker que hace que sea más fácil almacenar y usar credenciales de Docker cuando se insertan y se extraen imágenes de Amazon ECR. Para obtener

información sobre los pasos de instalación y configuración, consulte Amazon ECR Docker Credential Helper.

Usar un token de autorización

El ámbito de permiso de un token de autorización es igual que el de la entidad de seguridad de IAM que se utiliza para recuperar dicho token. Los tokens de autenticación se utilizan para acceder a un registro de Amazon ECR al que la entidad de seguridad de IAM tiene acceso y que es válido durante 12 horas. Para obtener un token de autorización, debe usar la operación GetAuthorizationToken de la API para recuperar un token de autorización codificado en base64 que contenga el nombre de usuario `AWS` y una contraseña codificada. Con el comando `get-login-password` de la AWS CLI, este proceso resulta más sencillo, ya que recupera y descodifica el token de autorización, que después puede canalizarse a un comando docker login para realizar la autenticación.

Para autenticar Docker en un registro privado de Amazon ECR con get-login-password

Para autenticar Docker en un registro de Amazon ECR con get-login-password, ejecute el comando aws ecr get-login-password. Al pasar el token de autenticación al comando docker login, utilice el valor `AWS` para el nombre de usuario y especifique el URI del registro de Amazon ECR en el que desea autenticarse. Si se autentica en varios registros, deberá repetir el comando con cada registro.

> **Important**
>
> Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

- get-login-password (AWS CLI)

```
aws ecr get-login-password --region region | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

- Get-ECRLoginCommand (Herramientas de AWS para Windows PowerShell)

```
(Get-ECRLoginCommand).Password | docker login --username AWS --password-
stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

Para autenticar Docker en un registro privado de Amazon ECR con get-login

Cuando se utilizan versiones de AWS CLI anteriores a la 1.17.10, el comando get-login está disponible para autenticarse en su registro de Amazon ECR. Puede comprobar la versión de la AWS CLI con el comando aws --version.

1. Ejecute el comando aws ecr get-login. El ejemplo siguiente se aplica al registro predeterminado asociado con la cuenta que realiza la solicitud. Para tener acceso a otros registros de la cuenta, utilice la opción `--registry-ids` *aws_account_id*. Para obtener más información, consulte get-login en la AWS CLI Command Reference.

   ```
   aws ecr get-login --region region --no-include-email
   ```

   El resultado es un comando docker login de Docker que se utiliza para autenticar el cliente Docker en el registro de Amazon ECR.

   ```
   docker login -u AWS -p password https://aws_account_id.dkr.ecr.region.amazonaws.com
   ```

2. Copie y pegue el comando docker login en un terminal para autenticar su CLI de Docker en el registro. Este comando proporciona un token de autorización que es válido durante 12 horas para el registro especificado.

   Note

   Si utiliza Windows PowerShell, no podrá copiar ni pegar cadenas largas como esta. Utilice el siguiente comando en su lugar.

   ```
   Invoke-Expression -Command (Get-ECRLoginCommand -Region region).Command
   ```

   Important

   Si ejecuta este comando docker login, otros usuarios del sistema podrán ver la cadena del comando en una pantalla de lista de procesos (ps -e). Como el comando docker login contiene las credenciales de autenticación, existe el riesgo de que otros usuarios de su sistema puedan verlas y usarlas para obtener acceso de recepción y envío a sus repositorios. Pueden usar las credenciales para obtener acceso de recepción y envío a sus repositorios. Si no se encuentra en un sistema seguro, deberá considerar este riesgo e iniciar sesión de forma interactiva omitiendo la opción `-p password` y después introducir la contraseña cuando se le solicite.

Uso de la autenticación de la API de HTTP

Amazon ECR es compatible con la API HTTP de Docker Registry. Sin embargo, como Amazon ECR es un registro privado, debe proporcionar un token de autorización con cada solicitud HTTP. Puede añadir un encabezado de autorización HTTP con la opción `-H` de curl para curl y pasar el código de autorización que proporciona el comando de la AWS CLI get-authorization-token.

Para autenticar con la API HTTP de Amazon ECR

1. Recupere un token de autorización con la AWS CLI y establézcalo en una variable de entorno.

   ```
   TOKEN=$(aws ecr get-authorization-token --output text --query
    'authorizationData[].authorizationToken')
   ```

2. Para autenticarse en la API, pase la variable `$TOKEN` a la opción `-H` de curl. Por ejemplo, el siguiente comando muestra las etiquetas de imagen en un repositorio de Amazon ECR. Para obtener más información, consulte la documentación de referencia de la API HTTP de Docker Registry.

   ```
   curl -i -H "Authorization: Basic $TOKEN"
    https://aws_account_id.dkr.ecr.region.amazonaws.com/v2/amazonlinux/tags/list
   ```

   La salida es la siguiente:

   ```
   HTTP/1.1 200 OK
   Content-Type: text/plain; charset=utf-8
   Date: Thu, 04 Jan 2018 16:06:59 GMT
   Docker-Distribution-Api-Version: registry/2.0
   Content-Length: 50
   Connection: keep-alive

   {"name":"amazonlinux","tags":["2017.09","latest"]}
   ```

Configuración de registros privados

Amazon ECR utiliza la configuración del registro para configurar características en el nivel del registro. Los ajustes del registro privado se configuran por separado para cada región. En la actualidad, la única configuración del registro es la configuración de replicación, que se utiliza para configurar la replicación entre regiones y entre cuentas de las imágenes en los repositorios.

Temas

Configuración de replicación

Se puede configurar un registro de Amazon ECR para la replicación entre regiones o entre cuentas. La replicación se configura para un registro por separado para cada región. A continuación se describen los métodos de replicación admitidos con más detalle:

Replicación entre regiones

La habilitación de la replicación entre regiones para su registro realiza copias de los repositorios en una o varias regiones de destino. Solo se copian las imágenes insertadas en un repositorio una vez configurada la replicación entre regiones.

Replicación entre cuentas

El habilita la replicación entre cuentas para su registro realiza copias de los repositorios de la cuenta de destino y de las regiones que especifique. Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro para permitir que se produzca la replicación desde su registro. Para obtener más información, consulte Permisos de registro privado (p. 20).

Consideraciones para la replicación de registros privados

Al utilizar la replicación de registros privados, se debe tener en cuenta lo siguiente.

- La primera vez que configure el registro privado para la replicación, Amazon ECR crea un rol vinculado al servicio en su nombre. El rol vinculado al servicio concede al servicio de replicación de Amazon ECR el permiso que necesita para crear repositorios y replicar imágenes en el registro. Para obtener más información, consulte Uso de roles vinculados a servicios de Amazon ECR (p. 80).
- Para que se produzca la replicación entre cuentas, el registro privado de destino debe conceder permiso para permitir que el registro de origen replique sus imágenes. Para obtener más información, consulte Permisos de registro privado (p. 20).
- Si los permisos de un registro se cambian para eliminar un permiso, cualquier replicación en curso concedida anteriormente puede completarse.
- Una acción de replicación solo se produce una vez por inserción de imagen. Por ejemplo, si ha configurado la replicación entre regiones de `us-west-2` a `us-east-1` y de `us-east-1` a `us-east-2`, una imagen enviada a `us-west-2` se replicará solo en `us-east-1`, no se replicará de nuevo en `us-east-2`. Este comportamiento se aplica tanto a la replicación entre regiones como entre cuentas.
- La replicación del registro no realiza ninguna acción de eliminación. Las imágenes replicadas y los repositorios se pueden eliminar manualmente cuando ya no se estén utilizando.
- La configuración del repositorio no se replica. La configuración de inmutabilidad de etiquetas, escaneo de imágenes y cifrado KMS se deshabilita de forma predeterminada en todos los repositorios creados por una acción de replicación. La configuración de inmutabilidad de etiquetas y escaneo de imágenes

se puede cambiar después de crear el repositorio. Sin embargo, la configuración solo se aplica a las imágenes enviadas después de que la configuración haya cambiado.

- Si se habilita la inmutabilidad de etiquetas en un repositorio y se replica una imagen que utiliza la misma etiqueta que una imagen existente, la imagen se replica pero no contiene la etiqueta duplicada. Esto podría dar lugar a que la imagen no se etiquete.

Configuración de los ajustes del registro privado

Los ajustes del registro se configuran por separado para cada región. Para obtener más información sobre la configuración de registro disponible, consulte Configuración de registros privados (p. 17).

Utilice los siguientes pasos para configurar los ajustes del registro.

Para configurar los ajustes del registro privado (Consola de administración de AWS)

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, elija la región para la que desea configurar los ajustes del registro.
3. En el panel de navegación, elija Registries (Registros).
4. En la página Registries (Registros), seleccione el registro Private (Privado) y elija Edit (Editar).
5. En la página Edit registry (Editar registro), haga lo siguiente.

   a. En Cross-Region replication (Replicación entre regiones), elija la configuración de replicación entre regiones para el registro. Si se establece en Enabled (Habilitado), elija una o varias Regiones de destino.

   b. En Cross-account replication (Replicación entre cuentas), elija la configuración de replicación entre cuentas para el registro. Si se establece en Enabled (Habilitado), escriba el ID de la cuenta de destino y una o varias Regiones de destino en las que se replicará.

      Important

      Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro para permitir que se produzca la replicación. Para obtener más información, consulte Permisos de registro privado (p. 20).
6. Seleccione Save.

Para configurar los ajustes del registro privado (AWS CLI)

1. Cree un archivo JSON que contenga las opciones de configuración de replicación que va a definir para su registro. Esto podría contener una o varias reglas, cada una de las cuales contendrá una región y una cuenta de destino. Si desea que replique las imágenes en su propio registro entre regiones, especifique su propio ID de cuenta. Para obtener más ejemplos, consulte Ejemplos de configuración de registros privados (p. 19).

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "destination_region",
                    "registryId": "destination_accountId"
                }
            ]
        }
    ]
}
```

2. Cree una configuración de replicación para su registro.

```
aws ecr put-replication-configuration \
     --replication-configuration file://crr-setup.json \
     --region us-west-2
```

3. Confirme la configuración del registro.

```
aws ecr describe-registry \
     --region us-west-2
```

Ejemplos de configuración de registros privados

Los siguientes ejemplos muestran cómo se puede utilizar la configuración del registro.

Ejemplo: Configuración de la replicación entre regiones en una única región de destino

A continuación se muestra un ejemplo de configuración de la replicación entre regiones dentro de un único registro. En este ejemplo se supone que su ID de cuenta es `111122223333` y que está especificando esta configuración de replicación en una región distinta de `us-west-2`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
    ]
}
```

Ejemplo: Configuración de la replicación entre regiones en varias regiones de destino

A continuación se muestra un ejemplo de configuración de la replicación entre regiones dentro de un único registro. En este ejemplo se presupone que su ID de cuenta es `111122223333` y que está especificando esta configuración de replicación en una región distinta de `us-west-1` o `us-west-2`.

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-1",
                    "registryId": "111122223333"
                },
                {
                    "region": "us-west-2",
                    "registryId": "111122223333"
                }
            ]
        }
```

```
    ]
}
```

Ejemplo: Configuración de la replicación entre cuentas

A continuación se muestra un ejemplo de configuración de replicación entre cuentas para su registro. Este ejemplo configura la replicación en la cuenta de `444455556666` y en la región `us-west-2`.

> **Important**
>
> Para que se produzca la replicación entre cuentas, la cuenta de destino debe configurar una política de permisos de registro para permitir que se produzca la replicación. Para obtener más información, consulte Permisos de registro privado (p. 20).

```
{
    "rules": [
        {
            "destinations": [
                {
                    "region": "us-west-2",
                    "registryId": "444455556666"
                }
            ]
        }
    ]
}
```

Permisos de registro privado

Amazon ECR utiliza una política de registro para conceder permisos a una entidad principal de AWS, lo que permite la replicación de los repositorios de un registro de origen a su registro. De forma predeterminada, tiene permiso para configurar la replicación entre regiones en su propio registro. Solo tiene que configurar la política de registro si concede permiso a otra cuenta para replicar contenido en su registro.

Una política de registro debe conceder permiso para la acción de la API `ecr:ReplicateImage`. : esta API es una API interna de Amazon ECR que puede replicar imágenes entre regiones o cuentas. También puede conceder permiso para el permiso `ecr:CreateRepository`, lo que permite a Amazon ECR crear repositorios en su registro si no existen todavía. Si no se proporciona el permiso `ecr:CreateRepository`, se debe crear manualmente en el registro un repositorio con el mismo nombre que el repositorio de origen. Si ninguno de ellos termina, la replicación genera un error. Aparecen en CreateRepository todas las acciones erróneas de la API de ReplicateImage o CloudTrail.

Temas

- Configuración de una instrucción de permiso de registro privado (p. 20)
- Eliminación de una instrucción de permiso de registro privado (p. 22)
- Ejemplos de políticas de registro privadas (p. 22)

Configuración de una instrucción de permiso de registro privado

Puede añadir o actualizar la política de permisos del registro mediante los pasos siguientes. Puede añadir varias instrucciones de política por registro. Para ver ejemplos de políticas de , consulte Ejemplos de políticas de registro privadas (p. 22).

Para configurar una política de permisos para un registro privado (Consola de administración de AWS)

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En la barra de navegación, elija la región en la que desea configurar su política de registro.
3. En el panel de navegación, elija Registries (Registros).
4. En la página Registries (Registros), seleccione el registro Private (Privado) y elija Permissions (Permisos).
5. En la página Private registry permissions (Permisos de registro privado), elija Generate statement (Generar instrucción).
6. Siga los pasos que se describen a continuación para definir la instrucción de política mediante el generador de políticas.
   a. En Policy type (Tipo de política), elija Cross-account policy (Política entre cuentas).
   b. En Statement ID (ID de instrucción), escriba un ID de instrucción único. Este campo se utiliza como `Sid` en la política de registro.
   c. En Accounts (Cuentas), escriba la cuenta IDs de cada cuenta a la que desea conceder permisos. Al especificar varias cuentas IDs, sepárelas con una coma.
7. Amplíe la sección Preview policy statement para revisar la instrucción de política de permisos del registro.
8. Una vez confirmada la instrucción de la política, elija Add to policy para guardar la política en su registro.

Para configurar una política de permisos para un registro privado (AWS CLI)

1. Cree un archivo llamado `registry_policy.json` y rellénelo con una política de registro.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

2. Cree la política de registro utilizando el archivo de política.

```
aws ecr put-registry-policy \
      --policy-text file://registry_policy.json \
      --region us-west-2
```

3. Recupere la política para que la confirme su registro.

```
aws ecr get-registry-policy \
```

```
    --region us-west-2
```

Eliminación de una instrucción de permiso de registro privado

Puede eliminar todas las instrucciones de política de permisos del registro mediante los pasos siguientes.

Para eliminar una política de permisos de un registro privado (Consola de administración de AWS)

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En la barra de navegación, elija la región en la que desea configurar la política de permisos del registro.
3. En el panel de navegación, elija Registries (Registros).
4. En la página Registries (Registros), seleccione el registro Private (Privado) y elija Permissions (Permisos).
5. En la página Private registry permissions (Permisos de registro privado), elija Delete (Eliminar).
6. En la pantalla de confirmación Delete registry policy, elija Delete policy.

Para eliminar una política de permisos de un registro privado (AWS CLI)

1. Elimine la política de registro.

```
aws ecr delete-registry-policy \
     --region us-west-2
```

2. Recupere la política para que la confirme su registro.

```
aws ecr get-registry-policy \
     --region us-west-2
```

Ejemplos de políticas de registro privadas

Los siguientes ejemplos muestran instrucciones de políticas de permisos de registro que puede utilizar para controlar los permisos que los usuarios tienen en su registro de Amazon ECR.

Ejemplo: Permitir que el usuario raíz de una cuenta de origen replique todos los repositorios

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
```

```
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

Ejemplo: Permitir varias cuentas

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        },
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

Ejemplo: Permitir al usuario raíz de una cuenta de origen replicar todos los repositorios a partir de `prod-`

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/prod-*"
```

```
            ]
        }
    ]
}
```

Ejemplo: Permitir al usuario raíz de una cuenta de origen replicar todos los repositorios a partir de `prod-`

Si la acción `ecr:CreateRepository` se elimina de la instrucción de permiso del registro, puede replicar los repositorios. Sin embargo, para que la replicación se realice correctamente, debe crear repositorios con el mismo nombre en su cuenta de .

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"ReplicationAccessCrossAccount",
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn:aws:iam::source_account_id:root"
            },
            "Action":[
                "ecr:ReplicateImage"
            ],
            "Resource": [
                "arn:aws:ecr:us-west-2:your_account_id:repository/*"
            ]
        }
    ]
}
```

Repositorios privados deAmazon ECR

Amazon EC2 Container Registry (Amazon ECR) proporciona operaciones de API para crear, monitorizar y eliminar repositorios de imágenes, así como para definir permisos que controlen quién puede tener acceso a ellos. Puede realizar las mismas acciones en la sección Repositories (Repositorios) de la consola de Amazon ECR. Amazon ECR también se integra con la CLI de Docker para insertar y extraer imágenes de los entornos de desarrollo en los repositorios.

Temas

Conceptos del repositorio

- De forma predeterminada, su cuenta tiene acceso de lectura y escritura en los repositorios e imágenes que cree en el registro predeterminado (`aws_account_id.dkr.ecr.region.amazonaws.com`). Sin embargo, los usuarios de IAM necesitan permisos para realizar llamadas al Amazon ECR APIs y para insertar o extraer imágenes en o de sus repositorios. Amazon ECR proporciona varias políticas administradas para controlar el acceso de los usuarios en diferentes niveles. Para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).
- Los repositorios se pueden controlar mediante políticas de acceso de usuarios de IAM y políticas de repositorio individuales. Para obtener más información, consulte Políticas de repositorio (p. 29).
- Los nombres de repositorio pueden admitir espacios de nombres, que puede usar para agrupar repositorios similares. Por ejemplo, si hay varios equipos que utilizan el mismo registro, el equipo A puede utilizar el espacio de nombres `team-a` y el equipo B puede utilizar el espacio de nombres `team-b`. Al hacerlo, cada equipo de `web-app` recibe su propia imagen llamada con cada imagen precedida por el espacio de nombres del equipo. Esta configuración permite que estas imágenes de cada equipo se utilicen simultáneamente sin interferencias. La imagen del equipo A es `team-a/web-app` y la imagen del equipo B es `team-b/web-app`.
- Las imágenes se pueden replicar en otros repositorios de entre regiones de su propio registro y entre cuentas de . Para ello, especifique una configuración de replicación en la configuración del registro. Para obtener más información, consulte Configuración de replicación (p. 17).

Creación de un repositorio

Antes de insertar sus imágenes de Docker en Amazon ECR, debe crear un repositorio para almacenarlas. Puede crear repositorios de Amazon ECR con la Consola de administración de AWS o con la AWS CLI y AWS SDKs.

Para crear un repositorio de

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región en la que va a crear el repositorio.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories, seleccione Create repository.
5. En Repository name (Nombre del repositorio), escriba un nombre único para el repositorio. El nombre del repositorio puede especificarse por sí solo (por ejemplo, `nginx-web-app`). También se puede anteponer un espacio de nombres para agrupar el repositorio en una categoría (por ejemplo, `project-a/nginx-web-app`).

   Note

   El nombre debe comenzar por una letra y solo puede contener letras minúsculas, números, guiones (-), guiones bajos (_) y barras diagonales (/).
6. En Tag mutability (Mutabilidad de etiquetas), seleccione la configuración de mutabiilidad de etiquetas del repositorio. Los repositorios configurados con etiquetas inmutables impiden que las etiquetas de imagen se sobrescriban. Para obtener más información, consulte Mutabilidad de etiquetas de imágenes (p. 58).
7. En Scan on push (Escanear al insertar), elija la configuración de escaneo de imágenes para el repositorio. Los repositorios que están configurados para escanear al insertar inician el escaneo de una imagen cada vez que se inserta una imagen. Si desea iniciar un escaneo de imagen en otro momento, debe iniciar manualmente los escaneos de imagen. Para obtener más información, consulte Escaneo de imágenes (p. 59).
8. En KMS encryption (Cifrado de KMS), elija si desea habilitar el cifrado de las imágenes en el repositorio mediante AWS Key Management Service. De forma predeterminada, cuando el cifrado de KMS está habilitado, Amazon ECR utiliza una clave maestra del cliente (CMK) administrada por AWS con el alias `aws/ecr`. Esta clave maestra se crea en su cuenta la primera vez que crea un repositorio con el cifrado de KMS habilitado. Para obtener más información, consulte Cifrado en reposo (p. 89).
9. Cuando el cifrado de KMS esté habilitado, seleccione Customer encryption settings (advanced) (Configuración de cifrado de cliente (avanzada)) para elegir su propia CMK. El CMK debe estar en la misma región que el clúster. Seleccione Create an AWS KMS key para ir a la consola de AWS KMS y crear su propia clave.
10. Elija Create repository.
11. (Opcional) Seleccione el repositorio que ha creado y elija View push commands (Ver comandos de inserción) para ver los pasos para insertar una imagen en el nuevo repositorio.

    a. Recupere el comandodocker login que puede utilizar para autenticar su cliente Docker en el registro pegando el comando aws ecr get-login desde la consola en una ventana de terminal.

       Note

       El comando get-login está disponible en la AWS CLI; a partir de 1.9.15; no obstante, le recomendamos la versión 1.11.91 o posterior para las versiones recientes de Docker (17.06 o posterior). Puede comprobar la versión de la AWS CLI con el comando aws --version. Si utiliza Docker versión 17.06 o posterior, incluya la opción `--no-include-email` después de `get-login`. Si recibe un error `Unknown options: --no-include-email`, instale la última versión de AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

    b. Ejecute el comando docker login que se devolvió en el paso anterior. Este comando proporciona un token de autorización que es válido durante 12 horas.

Important

Si ejecuta este comando docker login, otros usuarios del sistema podrán ver la cadena del comando en una pantalla de lista de procesos (ps -e). Como el comando docker login contiene las credenciales de autenticación, existe el riesgo de que otros usuarios de su sistema puedan verlas y usarlas para obtener acceso de recepción y envío a sus repositorios. Pueden usar las credenciales para obtener acceso de recepción y envío a sus repositorios. Si no se encuentra en un sistema seguro, deberá considerar este riesgo e iniciar sesión de forma interactiva omitiendo la opción `-p` *`password`* y después introducir la contraseña cuando se le solicite.

c. (Opcional) Si tiene un Dockerfile para la imagen que va a insertar, compile la imagen y etiquétela para su nuevo repositorio: pegando el comando docker build de la consola en una ventana de terminal. Asegúrese de que se encuentra en el mismo directorio que su Dockerfile.

d. Etiquete la imagen para su nuevo repositorio y registro de ECR pegando el comando docker tag desde la consola en una ventana de terminal. El comando de la consola presupone que la imagen se creó desde un Dockerfile en el paso anterior; si no creó la imagen desde un Dockerfile, sustituya la primera instancia de *`repository`*`:latest` por el ID o el nombre de imagen de la imagen local que desea insertar.

e. Inserte la imagen recién etiquetada en su repositorio de ECR pegando el comando docker push en una ventana de terminal.

f. Elija Close (Cerrar).

Visualización de la información del repositorio

Después de crear un repositorio, puede ver su información en la Consola de administración de AWS:

- Las imágenes que se almacenan en un repositorio
- Si una imagen se etiqueta
- Las etiquetas de la imagen
- El resumen SHA de las imágenes
- El tamaño de las imágenes en MiB.
- Si la imagen se insertó en el repositorio

Note

A partir de la versión 1.9 de Docker, el cliente Docker comprime capas de imágenes antes de insertarlas en un registro de Docker V2. El resultado del comando docker images muestra el tamaño de la imagen sin comprimir. Por lo tanto, tenga en cuenta que Docker podría devolver una imagen de mayor tamaño que la imagen que se muestra en la Consola de administración de AWS.

Para ver la información del repositorio (Consola de administración de AWS)

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio que desea ver.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories, elija el repositorio que desea ver.
5. En los repositorios de : ***`repository_name`***, utilice la barra de navegación para ver información sobre una imagen.

- Elija Images (Imágenes) para ver información sobre las imágenes del repositorio. Para ver más información sobre la imagen, seleccione la imagen. Para obtener más información, consulte Visualización de detalles de la imagen (p. 43).

  Si hay imágenes sin etiquetar que desee eliminar, puede seleccionar la casilla situada a la izquierda de los repositorios que desea eliminar y elegir Delete (Eliminar). Para obtener más información, consulte Eliminar una imagen (p. 44).
- Elija Permissions (Permisos) para ver las políticas de repositorio que se aplican al repositorio. Para obtener más información, consulte Políticas de repositorio (p. 29).
- Elija Lifecycle Policy (Política de ciclo de vida) para ver las reglas de política de ciclo de vida que se aplican al repositorio. El historial de eventos del ciclo de vida también se visualiza aquí. Para obtener más información, consulte Políticas de ciclo de vida (p. 47).
- Elija Tags (Etiquetas) para ver las etiquetas de metadatos que se aplican al repositorio.

Edición de un repositorio

Los repositorios existentes se pueden editar para cambiar la mutabilidad de las etiquetas de imagen y la configuración de escaneo de imágenes.

Para editar un repositorio

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, elija la región que contiene el repositorio que desea editar.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories (Repositorios), seleccione el repositorio que desea editar y haga clic en Edit (Editar).
5. En Tag mutability (Mutabilidad de etiquetas), seleccione la configuración de mutabiilidad de etiquetas del repositorio. Los repositorios configurados con etiquetas inmutables impiden que las etiquetas de imagen se sobrescriban. Para obtener más información, consulte Mutabilidad de etiquetas de imágenes (p. 58).
6. En Scan on push (Escanear al insertar), elija la configuración de escaneo de imágenes para el repositorio. Los repositorios configurados para escanear al insertar inician un escaneo de imagen cada vez que se inserta una imagen. Si desea que los escaneos de imágenes comiencen a una hora diferente, debe iniciarlos manualmente. Para obtener más información, consulte Escaneo de imágenes (p. 59).
7. Seleccione Save (Guardar) para actualizar la configuración del repositorio.

Eliminación de un repositorio

Si ha terminado de utilizar un repositorio, puede eliminarlo. Cuando elimina un repositorio en la Consola de administración de AWS, todas las imágenes incluidas en él se eliminan también, y esta acción no se puede deshacer.

Para eliminar un repositorio

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio que desea eliminar.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories (Repositorios), seleccione el repositorio que desea eliminar y elija Delete (Eliminar).

5. En el cuadro de diálogo Delete (Eliminar) ***repository_name***, verifique que los repositorios seleccionados se deben eliminar y elija Delete.

   Important

   Se eliminan también todas las imágenes de los repositorios seleccionados.

Políticas de repositorio

Amazon ECR utiliza permisos basados en recursos para controlar el acceso a los repositorios. Los permisos basados en recursos le permiten especificar qué usuarios o roles de IAM tienen acceso a un repositorio y qué acciones pueden realizar en él. De forma predeterminada, solo el propietario del repositorio tiene acceso a él. Puede aplicar un documento de política que permita permisos adicionales en su repositorio.

Políticas de repositorio frente a IAM políticas

Amazon ECR las políticas de repositorio son un subconjunto de IAM políticas para las que se utiliza y se utilizan específicamente para controlar el acceso a la persona Amazon ECR repositorios. IAM generalmente se utilizan para aplicar permisos para todo el Amazon ECR servicio, pero también se puede utilizar para controlar el acceso a recursos específicos.

Ambos Amazon ECR políticas de repositorio y IAM se utilizan a la hora de determinar qué acciones se aplican IAM el usuario o la función pueden realizar en un repositorio. Si se le permite realizar una acción a un rol o usuario mediante una política de repositorio, pero el permiso se deniega mediante una política de IAM (o viceversa), la acción se denegará. Un usuario o rol únicamente necesita que se le conceda permiso para realizar una acción mediante una política de repositorio o una política de IAM, pero no mediante ambas.

Important

Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Puede utilizar cualquiera de estos tipos de política para controlar el acceso a los repositorios, como se muestra en los siguientes ejemplos.

Este ejemplo muestra un ejemplo Amazon ECR política de repositorio, que permite un IAM usuario para describir el repositorio y las imágenes del repositorio.

```
{
  "Version": "2008-10-17",
  "Statement": [{
    "Sid": "ECR Repository Policy",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::account-id:user/username"
    },
    "Action": [
       "ecr:DescribeImages",
       "ecr:DescribeRepositories"
    ]
  }]
```

```
}
```

En este ejemplo se muestra una política de IAM que logra el mismo objetivo que la anterior al limitar la política a un repositorio (especificado por el ARN completo del repositorio) mediante el parámetro de recurso. Para obtener más información sobre el formato de Nombres de recursos de Amazon (ARN), consulte Resources (p. 76).

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "ECR Repository Policy",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::account-id:user/username"
    },
    "Action": [
      "ecr:DescribeImages",
      "ecr:DescribeRepositories"
    ],
    "Resource": [
      "arn:aws:ecr:region:account-id:repository/repository-name"
    ]
    }]
}
```

Temas

- Establecer una declaración de política de repositorio (p. 30)
- Eliminar una declaración de política de repositorio (p. 31)
- Ejemplos de políticas de repositorio (p. 31)

Establecer una declaración de política de repositorio

Puede añadir una instrucción de política de acceso a un repositorio en la Consola de administración de AWS mediante los pasos que se describen a continuación. Puede añadir varias instrucciones de política por repositorio. Para ver ejemplos de políticas de , consulte Ejemplos de políticas de repositorio (p. 31).

> **Important**
>
> Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Para definir una instrucción de política de repositorio

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio para el que desea definir una instrucción de política.
3. En el panel de navegación, seleccione Repositorios.
4. En el Repositorios seleccione el repositorio para establecer una declaración de directiva en.
5. En el panel de navegación, seleccione Permisos, , Editar.
6. En el Editar permisos página, elegir Añadir extracto.
7. Para Nombre de extracto, introduzca un nombre para la afirmación.

8. Para Efecto, elegir si la declaración de la póliza dará lugar a una denegación o a una denegación explícita.
9. Para Principal, elegir el alcance para aplicar la declaración de la póliza a. Para obtener más información, consulte Elementos de la política de AWS JSON: Principal en el Guía del usuario de IAM.

   - Puede aplicar la declaración a todas las autenticadas AWS usuarios seleccionando el Todos (*) casilla de verificación.
   - Para Principal de servicio, especifique el nombre del principal de servicio (por ejemplo, `ecs.amazonaws.com`) para aplicar la declaración a un servicio específico.
   - Para ID de cuenta de AWS, especificar un AWS número de cuenta (por ejemplo, `111122223333`) para aplicar la declaración a todos los usuarios de un AWS cuenta. Se pueden especificar varias cuentas utilizando una lista delimitada por comas.
   - Para IAM Entidades, seleccione los roles o usuarios de su AWS cuenta para aplicar la declaración a.

     Note

     Para políticas de repositorio más complejas no admitidas actualmente en la Consola de administración de AWS, puede aplicar la política con el comando de la AWS CLI set-repository-policy.
10. Para Acciones, elegir el alcance de la Amazon ECR Operaciones de API que la declaración de política debe aplicarse a partir de la lista de operaciones de API individuales.
11. Cuando haya terminado, elija Guardar para establecer la política.
12. Repita el paso anterior para cada política de repositorio que desee añadir.

Eliminar una declaración de política de repositorio

Si ya no desea que una instrucción de política de repositorio existente se aplique a un repositorio, puede eliminarla.

Para eliminar una instrucción de política de repositorio

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio del que desea eliminar una instrucción de política.
3. En el panel de navegación, seleccione Repositorios.
4. En el Repositorios seleccione el repositorio para eliminar una declaración de directiva de.
5. En el panel de navegación, seleccione Permisos, , Editar.
6. En el Editar permisos página, elegir Eliminar.

Ejemplos de políticas de repositorio

Los siguientes ejemplos muestran las declaraciones de políticas que podría utilizar para controlar los permisos que tienen los usuarios Amazon ECR repositorios.

Important

Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Ejemplo. Permitir un IAM usuario dentro de su cuenta

La siguiente política de repositorio permite a los usuarios de IAM de su cuenta insertar y extraer imágenes.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "AllowPushPull",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:user/push-pull-user-1",
                    "arn:aws:iam::account-id:user/push-pull-user-2"
                ]
            },
            "Action": [
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "ecr:BatchCheckLayerAvailability",
                "ecr:PutImage",
                "ecr:InitiateLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:CompleteLayerUpload"
            ]
        }
    ]
}
```

Ejemplo. Permitir otra cuenta

La siguiente política de repositorio permite a una cuenta específica insertar imágenes.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "AllowCrossAccountPush",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": [
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchCheckLayerAvailability",
                "ecr:PutImage",
                "ecr:InitiateLayerUpload",
                "ecr:UploadLayerPart",
                "ecr:CompleteLayerUpload"
            ]
        }
    ]
}
```

La siguiente política de depósito permite IAM usuarios para extraer imágenes (*pull-user-1* y *pull-user-2*) al tiempo que proporciona acceso completo a otro (*admin-user*).

> **Note**
>
> Para políticas de repositorio más complejas no admitidas actualmente en la Consola de administración de AWS, puede aplicar la política con el comando de la AWS CLI set-repository-policy.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "AllowPull",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:user/pull-user-1",
                    "arn:aws:iam::account-id:user/pull-user-2"
                ]
            },
            "Action": [
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage"
            ]
        },
        {
            "Sid": "AllowAll",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:user/admin-user"
            },
            "Action": [
                "ecr:*"
            ]
        }
    ]
}
```

Ejemplo. Permitir todo AWS cuentas para extraer imágenes

La siguiente política de repositorio permite a todas las cuentas de AWS para extraer imágenes.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "AllowPull",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage"
            ]
        }
    ]
}
```

Ejemplo. Denegar todo

La siguiente política de repositorio deniega a todos los usuarios la capacidad de extraer imágenes.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "DenyPull",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
```

```
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage"
            ]
        }
    ]
}
```

Ejemplo. Restringir el acceso a direcciones IP específicas

En el siguiente ejemplo se conceden permisos a cualquier usuario para que realice operaciones de Amazon ECR en un repositorio. Sin embargo, la solicitud debe proceder del rango de direcciones IP especificado en la condición.

La condición en esta instrucción identifica el rango `54.240.143.*` de direcciones IP permitidas en formato de Protocolo de Internet versión 4 (IPv4), con una excepción: . `54.240.143.188`.

El `Condition` bloque utiliza el `IpAddress` y `NotIpAddress` y el `aws:SourceIp` clave de condición, que es una AWStecla de estado ancho. Para obtener más información sobre estas claves de condición, consulte AWS Claves de contexto de la condición global. Los valores de IPv4 `aws:sourceIp` utilizan la notación CIDR estándar. Para obtener más información, consulte Operadores de condición de dirección IP en el Guía del usuario de IAM.

```
{
    "Version": "2012-10-17",
    "Id": "ECRPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "ecr:*",
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "54.240.143.188/32"
                },
                "IpAddress": {
                    "aws:SourceIp": "54.240.143.0/24"
                }
            }
        }
    ]
}
```

Ejemplo. Rol vinculado al servicio

La siguiente política de depósito permite AWS CodeBuild acceso al Amazon ECR Acciones API necesarias para la integración con ese servicio. Para obtener más información, consulte Amazon ECR Muestra para CodeBuild en el Guía del usuario de AWS CodeBuild.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CodeBuildAccess",
            "Effect": "Allow",
            "Principal": {
                "Service": "codebuild.amazonaws.com"
            },
            "Action": [
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer"
```

```
            ]
        }
    ]
}
```

Etiquetado de un repositorio deAmazon ECR

Como ayuda para administrar los repositorios de Amazon ECR, puede asignar sus propios metadatos a cada repositorio en forma de etiquetas. En este tema se describe qué son las etiquetas y cómo crearlas.

Instancias de destino que están fuera de línea especificando un grupo de recursos de AWS como destino.Contenido

Conceptos básicos de etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario.

Las etiquetas le permiten clasificar los recursos de AWS de diversas maneras, por ejemplo, según su finalidad, propietario o entorno. Este es útil cuando tiene muchos recursos del mismo tipo — le permite identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado. Por ejemplo, podría definir un conjunto de etiquetas para los repositorios de Amazon ECR de su cuenta que le ayude a realizar un seguimiento del propietario de cada repositorio.

Le recomendamos que idee un conjunto de claves de etiqueta que cumpla sus necesidades. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos más fácilmente. Puede buscar y filtrar los recursos en función de las etiquetas que agregue.

Las etiquetas no tienen ningún significado semántico para Amazon ECR, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Puede trabajar con etiquetas utilizando la Consola de administración de AWS, la AWS CLI y la API de Amazon ECR.

Si utiliza AWS Identity and Access Management (IAM), puede controlar qué usuarios de su cuenta de AWS tienen permiso para crear, editar o eliminar etiquetas.

Etiquetado de los recursos de

Puede etiquetar repositorios de Amazon ECR nuevos o existentes.

Si utiliza la consola de Amazon ECR, puede aplicar etiquetas a los recursos de nueva creación o a los existentes mediante la opción Tags (Etiquetas) en el panel de navegación cuando lo desee.

Si utiliza la API de Amazon ECR, la AWS CLI o un SDK de AWS, puede aplicar etiquetas a los repositorios nuevos mediante el parámetro `tags` en la acción CreateRepository de la API o utilizar la acción `TagResource` de la API para aplicar etiquetas a los recursos existentes. Para obtener más información, consulte TagResource.

Además, si no se pueden aplicar etiquetas durante la creación del repositorio, se revierte el proceso de creación del repositorio. Esto garantiza que los repositorios se creen con etiquetas o, de lo contrario, no se creen y que ningún repositorio se quede jamás sin etiquetar. Al etiquetar los repositorios en el momento de su creación, se eliminar la necesidad de ejecutar scripts de etiquetado personalizados tras la creación del repositorio.

Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas de :

- Número máximo de etiquetas por repositorio: 50
- Para cada repositorio, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Longitud máxima de la clave – 128 caracteres Unicode en UTF-8
- Longitud máxima del valor – 256 caracteres Unicode en UTF-8
- Si se utiliza su esquema de etiquetado en múltiples servicios y recursos de , recuerde que otros servicios pueden tener restricciones sobre caracteres permitidos. Los caracteres permitidos generalmente son: letras, números y espacios representables en UTF-8, además de los siguientes caracteres: + - = . _ : / @.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No utilice el prefijo `aws:` para claves o valores; su uso está reservado para AWS. Las claves y valores de etiquetas que tienen este prefijo no se pueden editar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

Etiquetado de los recursos para facturación

Las etiquetas que agregue a sus repositorios de Amazon ECR son útiles a la hora de revisar la asignación de costos una vez que las habilite en el informe de uso y costos. Para obtener más información, consulte Informes de uso de Amazon ECR (p. 104).

Para ver el costo de los recursos combinados, puede organizar la información de facturación basada en los recursos que tienen los mismos valores de clave de etiqueta. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver el costo total de la aplicación en distintos servicios. Para obtener más información sobre la configuración de un informe de asignación de costos con etiquetas, consulte Informe de asignación de costos mensual en la Guía del usuario de AWS Billing and Cost Management.

> Note
>
> Si acaba de habilitar la realización de informes, los datos correspondientes al mes actual estarán disponibles para su visualización transcurridas 24 horas.

Uso de etiquetas mediante la consola

Con la consola de Amazon ECR puede administrar las etiquetas asociadas a los repositorios nuevos o existentes.

Al seleccionar un repositorio específico en la consola de Amazon ECR, puede ver las etiquetas seleccionando Tags (Etiquetas) en el panel de navegación.

Para agregar una etiqueta a un repositorio

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En la barra de navegación, seleccione la región que desea utilizar.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories, elija el repositorio que desea ver.
5. En los repositorios de : ***repository_name***, seleccione Tags en el panel de navegación.
6. En la pestaña Tags (Etiquetas), seleccione Add tags (Añadir etiquetas), Add tag (Añadir etiqueta).
7. En la página Edit Tags (Editar etiquetas), especifique la clave y el valor de cada etiqueta y, a continuación, elija Save (Guardar).

Para eliminar una etiqueta de un recurso individual

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En la barra de navegación, seleccione la región que desea utilizar.
3. En la página Repositories, elija el repositorio que desea ver.
4. En los repositorios de : ***repository_name***, seleccione Tags en el panel de navegación.
5. En la pestaña Tags (Etiquetas), seleccione Edit (Editar).
6. En la página Edit Tags (Editar etiquetas), seleccione Remove (Eliminar) para cada etiqueta que desee eliminar y, a continuación, elija Save (Guardar).

Uso de etiquetas mediante la AWS CLI o la API

Utilice lo siguiente para añadir, actualizar, listar y eliminar las etiquetas de los recursos. En la documentación correspondiente se proporcionan ejemplos.

Compatibilidad de etiquetado para recursos de Amazon ECR

Tarea	CLI de AWS	Acción API
Añadir o sobrescribir una o varias etiquetas.	tag-resource	TagResource
Eliminar una o varias etiquetas.	untag-resource	UntagResource

En los siguientes ejemplos se muestra cómo administrar las etiquetas con la AWS CLI.

Ejemplo 1: Etiquetado de un repositorio existente

El siguiente comando etiqueta un repositorio existente.

```
aws ecr tag-resource --resource-arn
 arn:aws:ecr:region:account_id:repository/repository_name --tags Key=stack,Value=dev
```

Ejemplo 2: Etiquetar un repositorio existente con varias etiquetas

El siguiente comando etiqueta un repositorio existente.

```
aws ecr tag-resource --resource-arn
 arn:aws:ecr:region:account_id:repository/repository_name --tags Key=key1,Value=value1
 Key=key2,Value=value2 Key=key3,Value=value3
```

Ejemplo 3: Elimina la etiqueta de un repositorio existente.

El siguiente comando elimina una etiqueta de un repositorio existente.

```
aws ecr untag-resource --resource-arn
 arn:aws:ecr:region:account_id:repository/repository_name --tag-keys tag_key
```

Ejemplo 4: Enumera las etiquetas de un repositorio.

El siguiente comando enumera las etiquetas asociadas a un repositorio existente.

```
aws ecr list-tags-for-resource --resource-arn
 arn:aws:ecr:region:account_id:repository/repository_name
```

Ejemplo 5: Crear un repositorio y aplicar una etiqueta

El siguiente comando crea un repositorio denominado `test-repo` y añade una etiqueta con clave `team` y valor `devs`.

```
aws ecr create-repository --repository-name test-repo --tags Key=team,Value=devs
```

Imágenes privadas

Amazon EC2 Container Registry (Amazon ECR) almacena imágenes de Docker, imágenes Open Container Initiative (OCI) y artefactos compatibles con OCI en repositorios de . Puede utilizar la CLI de Docker o su cliente preferido para insertar y extraer imágenes en y desde sus repositorios.

> **Important**
>
> Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Temas

Insertar una imagen

Puede insertar sus imágenes de Docker, listas de manifiesto e imágenes de Open Container Initiative (OCI) y artefactos compatibles en el repositorio. En las páginas siguientes se describen con más detalle.

> **Note**
>
> Las imágenes se pueden replicar en otros repositorios de entre regiones de su propio registro y entre cuentas especificando una configuración de replicación en su configuración de registro. Para obtener más información, consulte Configuración de replicación (p. 17).

Temas

Inserción de una imagen de Docker

Puede insertar sus imágenes de Docker en un repositorio de Amazon ECR con el comando docker push.

Important

Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

también admite la creación y el envío de listas de manifiestos de Docker, que se utilizan para imágenes multiarquitectura.Amazon ECR Cada imagen a la que se hace referencia en una lista de manifiesto ya debe haberse insertado en su repositorio. Para obtener más información, consulte Empujar una imagen multiarquitectura (p. 40).

Para insertar una imagen de Docker en un repositorio de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR en el que va a insertar la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).
2. Si el repositorio de imágenes no existe aún en el registro en el que lo va a insertar, créelo. Para obtener más información, consulte Creación de un repositorio (p. 25).
3. Identifique la imagen que va a insertar. Ejecute el comando docker images para mostrar las imágenes en el sistema.

   ```
   docker images
   ```

   Puede identificar una imagen con el *repository:tag* el valor o el ID de la imagen en la salida del comando resultante.
4. Etiquete su imagen con la combinación de registro, repositorio y etiqueta de imagen opcional de Amazon ECR que va a usar. El formato del registro es *aws_account_id*.dkr.ecr.*region*.amazonaws.com. El nombre del repositorio debe coincidir con el repositorio que ha creado para su imagen. Si omite la etiqueta de imagen, se presupone que la etiqueta es `latest`.

   El siguiente ejemplo etiqueta una imagen con el ID *e9ae3c220b23* como *aws_account_id*.dkr.ecr.*region*.amazonaws.com/my-web-app.

   ```
   docker tag e9ae3c220b23 aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app
   ```
5. Inserte la imagen mediante el comando docker push:

   ```
   docker push aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app
   ```
6. (Opcional) Aplique todas las demás etiquetas a su imagen e insértelas en Amazon ECR repitiendo Step 4 (p. 40) y Step 5 (p. 40). Puede aplicar hasta 100 etiquetas a cada imagen en Amazon ECR.

Empujar una imagen multiarquitectura

Amazon ECR admite la creación y el envío de listas de manifiesto de Docker, que se utilizan para imágenes multiarquitectura. Una lista de manifiesto es una lista de imágenes que se crea especificando uno o más nombres de imagen. En la mayoría de los casos, la lista de manifiestos se crea a partir de imágenes que sirven a la misma función, pero para diferentes sistemas operativos o arquitecturas. La lista de manifiestos no es obligatoria. Para obtener más información, consulte manifiesto de docker.

Important

La CLI de Docker debe tener funciones experimentales habilitadas para usar esta función. Para obtener más información, consulte Características experimentales.

Se puede extraer o hacer referencia a una lista de manifiesto en una definición de tarea de Amazon ECS o especificación de pod de Amazon EKS como otras imágenes de Amazon ECR.

Los siguientes pasos se pueden utilizar para crear y enviar una lista de manifiesto de Docker a un repositorio de Amazon ECR. Ya debe tener las imágenes enviadas a su repositorio para hacer referencia en el manifiesto de Docker. Para obtener información sobre cómo insertar una imagen, consulte Inserción de una imagen de Docker (p. 39).

Para insertar una imagen de Docker multiarquitectura a un repositorio de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR en el que desea insertar la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).
2. Enumere las imágenes en su repositorio, confirmando las etiquetas de imagen.

```
aws ecr describe-images --repository-name my-web-app
```

3. Cree la lista de manifiestos de Docker. El comando `manifest create` verifica que las imágenes a las que se hace referencia ya estén en su repositorio y crea el manifiesto localmente.

```
docker manifest create aws_account_id.dkr.ecr.region.amazonaws.com/my-
web-app aws_account_id.dkr.ecr.region.amazonaws.com/my-web-
app:image_one_tag aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app:image_two
```

4. (Opcional) Inspeccione la lista de manifiestos de Docker. Esto le permite confirmar el tamaño y la síntesis de cada manifiesto de imagen al que se hace referencia en la lista de manifiestos.

```
docker manifest inspect aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app
```

5. Impulse la lista de manifiestos de Docker en su repositorio de Amazon ECR.

```
docker manifest push aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app
```

Inserción de un gráfico de Helm

Amazon ECR admite el envío de artefactos Open Container Initiative (OCI) a los repositorios. Para mostrar esta funcionalidad, siga estos pasos para insertar un gráfico de Helm en Amazon ECR.

Para obtener más información sobre el uso de los gráficos de Helm alojados en Amazon ECR con Amazon EKS, consulte Instalación de un gráfico de timón alojado en Amazon ECR con Amazon EKS (p. 66).

Para insertar un gráfico de Helm en un repositorio deAmazon ECR

1. Instale el cliente de Helm versión 3. Para obtener más información, consulte Instalación de Helm.
2. Habilite la compatibilidad con OCI en el cliente de Helm 3.

```
export HELM_EXPERIMENTAL_OCI=1
```

3. Cree un repositorio para almacenar el gráfico de Helm. Para obtener más información, consulte Creación de un repositorio (p. 25).

```
aws ecr create-repository \
     --repository-name artifact-test \
     --region us-west-2
```

4. Autentique su cliente Helm en el registro de Amazon ECR en el que va a insertar el gráfico Helm. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).

```
aws ecr get-login-password \
     --region us-west-2 | helm registry login \
     --username AWS \
     --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

5. Siga estos pasos para crear un gráfico Helm de prueba. Para obtener más información, consulte Helm Docs - Getting Started.

   a. Cree un directorio llamado `helm-tutorial` para trabajar en él.

   ```
   mkdir helm-tutorial
   cd helm-tutorial
   ```

   b. Cree un gráfico Helm denominado `mychart` y borre el contenido del directorio `templates`.

   ```
   helm create mychart
   rm -rf ./mychart/templates/*
   ```

   c. Cree un ConfigMap en la carpeta `templates`.

   ```
   cd mychart/templates
   cat <<EOF > configmap.yaml
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: mychart-configmap
   data:
     myvalue: "Hello World"
   EOF
   ```

6. Guarde el gráfico localmente y cree un alias para el gráfico con su URI de registro.

```
cd ..
helm chart save . mychart
helm chart save . aws_account_id.dkr.ecr.us-west-2.amazonaws.com/artifact-test:mychart
```

7. Identifique el gráfico Helm que desea insertar. Ejecute el comando helm chart list para enumerar los gráficos Helm de su sistema.

```
helm chart list
```

El resultado debería tener un aspecto similar al siguiente:

```
REF                                                             NAME    VERSION DIGEST
 SIZE    CREATED
aws_account_id.dkr.ecr.us-west-2.amazonaws.com/artifact-tes..   mychart 0.1.0   30e0a03
 3.6 KiB 14 seconds
mychart                                                         mychart 0.1.0   ba3e62a 3.6
 KiB About a minute
```

8. Envíe el gráfico de Helm con el comando helm chart push:

```
helm chart push aws_account_id.dkr.ecr.region.amazonaws.com/artifact-test:mychart
```

9. Describa su gráfico de Helm.

```
aws ecr describe-images \
     --repository-name artifact-test \
     --region us-west-2
```

En la salida, verifique que el parámetro `artifactMediaType` indica el tipo de artefacto adecuado.

```
{
    "imageDetails": [
        {
            "registryId": "aws_account_id",
            "repositoryName": "artifact-test",
            "imageDigest":
 "sha256:f23ab9dc0fda33175e465bd694a5f4cade93eaf62715fa9390d9fEXAMPLE",
            "imageTags": [
                "mychart"
            ],
            "imageSizeInBytes": 3714,
            "imagePushedAt": 1597433021.0,
            "imageManifestMediaType": "application/vnd.oci.image.manifest.v1+json",
            "artifactMediaType": "application/vnd.cncf.helm.config.v1+json"
        }
    ]
}
```

Visualización de detalles de la imagen

Una vez que haya enviado una imagen al repositorio, puede ver su información en la Consola de administración de AWS. Los detalles que se incluyen son los siguientes:

- URI de imagen
- Etiquetas de imagen
- Tipo de medios del artefacto
- Tipo de manifiesto de imagen
- Estado de análisis
- El tamaño de la imagen en MB
- Si la imagen se insertó en el repositorio
- El estado de la replicación

Para ver los detalles de la imagen (Consola de administración de AWS)

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, elija la región que contiene el repositorio que contiene la imagen.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories, elija el repositorio que desea ver.
5. En los repositorios de : ***repository_name***, elija la imagen de la que desea ver los detalles.

Extraer una imagen

Si desea ejecutar una imagen de Docker que está disponible en Amazon ECR, puede extraerla a su entorno local con el comando docker pull. Puede hacerlo desde su registro predeterminado o desde un registro asociado a otra cuenta de AWS. Para utilizar una imagen de Amazon ECR en una definición de tarea de Amazon ECS, consulte .Uso de imágenes de Amazon ECR con Amazon ECS (p. 65).

> **Important**
>
> Amazon ECR requiere que se concedan a los usuarios permisos para la API `ecr:GetAuthorizationToken` a través de una política de IAM para que puedan autenticarse en un registro e insertar o extraer imágenes de cualquier repositorio de Amazon ECR. Amazon ECR proporciona varias políticas administradas de IAM para controlar el acceso de los usuarios a distintos niveles; para obtener más información, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Para extraer una imagen de Docker de un repositorio de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR del que va a extraer la imagen. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).
2. (Opcional) Identifique la imagen que va a extraer.
   - Puede mostrar los repositorios de un registro con el comando: aws ecr describe-repositories.

     ```
     aws ecr describe-repositories
     ```

     El registro de ejemplo anterior tiene un repositorio llamado `amazonlinux`.
   - Puede describir las imágenes de un repositorio con el comando: aws ecr describe-images.

     ```
     aws ecr describe-images --repository-name amazonlinux
     ```

     El repositorio de ejemplo anterior tiene una imagen etiquetada como `latest` y `2016.09`, con el resumen de imagen `sha256:f1d4ae3f7261a72e98c6ebefe9985cf10a0ea5bd762585a43e0700ed99863807`.
3. Extraiga la imagen con el comando docker pull. El formato del nombre de imagen debe ser *`registry`*`/`*`repository`*`[:`*`tag`*`]` para extraer la imagen por etiqueta o *`registry`*`/`*`repository`*`[@`*`digest`*`]` para extraerla por resumen.

   ```
   docker pull aws_account_id.dkr.ecr.us-west-2.amazonaws.com/amazonlinux:latest
   ```

   > **Important**
   >
   > Si recibe un error *`repository-url`* `not found: does not exist or no pull access`, es posible que tenga que autenticar su cliente de Docker con Amazon ECR. Para obtener más información, consulte Autenticación de registros privados (p. 14).

Eliminar una imagen

Si ha terminado de usar una imagen, puede eliminarla del repositorio. Puede eliminar una imagen con la Consola de administración de AWS o la AWS CLI.

Note

Si ha terminado con un repositorio, puede eliminar todo el repositorio y todas las imágenes que este contiene. Para obtener más información, consulte Eliminación de un repositorio (p. 28).

Para eliminar una imagen con la Consola de administración de AWS

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene la imagen que desea eliminar.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories, elija el repositorio del que contiene la imagen que desea eliminar.
5. En los repositorios de : ***repository_name***, seleccione la casilla situada a la izquierda de la imagen que desea eliminar y elija Delete.
6. En el cuadro de diálogo Delete image(s), verifique las imágenes seleccionadas que deben eliminarse y elija Delete.

Para eliminar una imagen con la AWS CLI

1. Muestre las imágenes del repositorio para identificarlas por etiqueta o resumen de imagen.

```
aws ecr list-images --repository-name my-repo
```

2. (Opcional) Elimine las etiquetas de la imagen que no desee especificando la etiqueta que desea eliminar.

   Note

   La imagen se elimina cuando elimina la última etiqueta.

```
aws ecr batch-delete-image --repository-name my-repo --image-ids imageTag=latest
```

3. Elimine la imagen especificando el resumen de la imagen que desea eliminar.

   Note

   Al eliminar una imagen haciendo referencia a su resumen, se elimina la imagen y todas sus etiquetas.

```
aws ecr batch-delete-image --repository-name my-repo --image-ids
 imageDigest=sha256:4f70ef7a4d29e8c0c302b13e25962d8f7a0bd304c7c2c1a9d6fa3e9de6bf552d
```

Volver a etiquetar una imagen

Con las imágenes de Docker Image Manifest V2 Schema 2 puede usar la opción `--image-tag` del comando put-image para volver a etiquetar una imagen existente. Puede volver a etiquetar sin extraer o insertar la imagen con Docker. Para imágenes grandes, este proceso ahorra una cantidad considerable de ancho de banda de red y del tiempo necesario para volver a etiquetar una imagen.

Para volver a etiquetar una imagen (AWS CLI)

Para volver a etiquetar una imagen con la AWS CLI

1. Use el comando batch-get-image para obtener el manifiesto de la imagen que va a volver a etiquetar y escribirlo en una variable de entorno. En este ejemplo, el manifiesto de una imagen con la etiqueta , *latest*, en el repositorio, *amazonlinux*, está escrito en la variable de entorno, *MANIFEST*.

```
MANIFEST=$(aws ecr batch-get-image --repository-name amazonlinux --image-ids
 imageTag=latest --query 'images[].imageManifest' --output text)
```

2. Use la opción `--image-tag` del comando put-image para colocar el manifiesto de la imagen en Amazon ECR con una nueva etiqueta. En este ejemplo, la imagen se etiqueta como . *2017.03*.

   Note

   Si la opción `--image-tag` no está disponible en su versión de la AWS CLI, actualice a la versión más reciente. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

```
aws ecr put-image --repository-name amazonlinux --image-tag 2017.03 --image-manifest
 "$MANIFEST"
```

3. Verifique que la nueva etiqueta de imagen está asociada a la imagen. En el siguiente resultado, la imagen tiene las etiquetas `latest` y `2017.03`.

```
aws ecr describe-images --repository-name amazonlinux
```

   La salida es la siguiente:

```
{
    "imageDetails": [
        {
            "imageSizeInBytes": 98755613,
            "imageDigest":
 "sha256:8d00af8f076eb15a33019c2a3e7f1f655375681c4e5be157a2685dfe6f247227",
            "imageTags": [
                "latest",
                "2017.03"
            ],
            "registryId": "aws_account_id",
            "repositoryName": "amazonlinux",
            "imagePushedAt": 1499287667.0
        }
    ]
}
```

Para volver a etiquetar una imagen (Herramientas de AWS para Windows PowerShell)

Para volver a etiquetar una imagen con la Herramientas de AWS para Windows PowerShell

1. Use el cmdlet Get-ECRImageBatch para obtener la descripción de la imagen que va a volver a etiquetar y escribirla en una variable de entorno. En este ejemplo, una imagen con la etiqueta , *latest*, en el repositorio, *amazonlinux*, está escrito en la variable de entorno, *$Image*.

   Note

   Si el cmdlet Get-ECRImageBatch no está disponible en su sistema, consulte Configuración de Herramientas de AWS para Windows PowerShell en la Guía del usuario de Herramientas de AWS para Windows PowerShell.

```
$Image = Get-ECRImageBatch -ImageId @{ imageTag="latest" } -RepositoryName amazonlinux
```

2. Escribir el manifiesto de la imagen en el *$Manifest* Variable de entorno .

```
$Manifest = $Image.Images[0].ImageManifest
```

3. Use la opción `-ImageTag` del cmdlet Write-ECRImage para colocar el manifiesto de la imagen en Amazon ECR con una nueva etiqueta. En este ejemplo, la imagen se etiqueta como . *2017.09*.

```
Write-ECRImage -RepositoryName amazonlinux -ImageManifest $Manifest -ImageTag 2017.09
```

4. Verifique que la nueva etiqueta de imagen está asociada a la imagen. En el siguiente resultado, la imagen tiene las etiquetas `latest` y `2017.09`.

```
Get-ECRImage -RepositoryName amazonlinux
```

La salida es la siguiente:

```
ImageDigest                                                             ImageTag
-----------                                                             --------
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 latest
sha256:359b948ea8866817e94765822787cd482279eed0c17bc674a7707f4256d5d497 2017.09
```

Políticas de ciclo de vida

Amazon ECRLas políticas de ciclo de vida de le permiten especificar la administración de ciclo de vida de las imágenes de un repositorio. Una política de ciclo de vida es un conjunto de una o más reglas, en la que cada regla define una acción de Amazon ECR. Las acciones se aplican a imágenes que contienen etiquetas con las cadenas especificadas como prefijo. Esto permite automatizar la limpieza de las imágenes sin utilizar, como las imágenes que deben marcarse para vencimiento en función de su edad o número. Una vez creada una política de ciclo de vida, las imágenes a las que afecta esta política caducan al cabo de 24 horas.

Temas

Plantilla de política de ciclo de vida

El contenido de la política de ciclo de vida se evalúa antes de asociarse a un repositorio. A continuación, se muestra la plantilla de sintaxis JSON de la política de ciclo de vida. Para ver ejemplos de política de ciclo de vida, consulte Ejemplos de políticas del ciclo de vida (p. 52).

```
{
    "rules": [
        {
            "rulePriority": integer,
            "description": "string",
            "selection": {
```

```
                "tagStatus": "tagged"|"untagged"|"any",
                "tagPrefixList": list<string>,
                "countType": "imageCountMoreThan"|"sinceImagePushed",
                "countUnit": "string",
                "countNumber": integer
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Note

El `tagPrefixList` solo se utiliza si `tagStatus` es `tagged`. El `countUnit` solo se utiliza si `countType` es `sinceImagePushed`. El `countNumber` solo se utiliza si `countType` está establecido en `imageCountMoreThan`.

Parámetros de la política del ciclo de vida

Las políticas de ciclo de vida se dividen en las siguientes partes:

Temas

Prioridad de regla

`rulePriority`

Tipo: número entero

Obligatorio: sí

Establece el orden en el que se evalúan las reglas, de menor a mayor. Una norma de política del ciclo de vida con una prioridad de `1` se actuará primero, una regla con prioridad de `2` será siguiente, y así sucesivamente. Cuando añada reglas a una política de ciclo de vida, debe darles cada valor único para `rulePriority`. No es necesario que los valores sean secuenciales en las reglas de una política. Una regla con un `tagStatus` valor de `any` debe tener el valor más alto para `rulePriority` y se evalúan los últimos.

Description

`description`

Tipo: string.

Obligatorio: No

(Opcional) Describe la finalidad de una regla de una política de ciclo de vida.

Estado de la etiqueta

`tagStatus`

Tipo: string.

Obligatorio: sí

Determina si la regla de la política de ciclo de vida que añade especifica una etiqueta para una imagen. Las opciones aceptables son `tagged`, , `untagged`, o `any`. Si especifica `any`, entonces todas las imágenes tienen la regla aplicada. Si especifica `tagged`, también debe especificar un `tagPrefixList` valor. Si especifica `untagged`, también debe omitir `tagPrefixList`.

Lista de prefijo de etiqueta

`tagPrefixList`

Tipo: lista[cadena]

Obligatorio: sí, solo si `tagStatus` está establecido en tagged

Solo se utiliza si ha especificado `"tagStatus": "tagged"`. Debe especificar una lista separada por comas de prefijos de etiqueta de imagen en los que se deben realizar acciones con la política del ciclo de vida. Por ejemplo, si sus imágenes se etiquetan como `prod`, , `prod1`, , `prod2`, y así sucesivamente, utilizaría el prefijo de etiquetas `prod` para especificar todos. Si especifica varias etiquetas, solo se seleccionan las imágenes con todas las etiquetas especificadas.

Tipo de recuento

`countType`

Tipo: string.

Obligatorio: sí

Especifique un tipo de recuento que desea aplicar a las imágenes.

Si `countType` está establecido en `imageCountMoreThan`, también especifica `countNumber` para crear una regla que establezca un límite en el número de imágenes que existen en el repositorio. Si `countType` está establecido en `sinceImagePushed`, también especifica `countUnit` y `countNumber` para especificar un límite de tiempo en las imágenes que existen en el repositorio.

Contar unidad

`countUnit`

Tipo: string.

Obligatorio: sí, solo si `countType` está establecido en `sinceImagePushed`

Especifique una unidad de recuento de `days` para indicar que, además de `countNumber`, que es el número de días.

Solo debe especificarse cuando `countType` es `sinceImagePushed` se producirá un error si especifica una unidad de recuento cuando `countType` es cualquier otro valor.

Cantidad

`countNumber`

Tipo: número entero

Obligatorio: sí

Especifique un número de recuento. Los valores aceptables son enteros positivos (el valor `0` no se acepta).

Si el `countType` usado es `imageCountMoreThan`, entonces el valor es el número máximo de imágenes que desea conservar en el repositorio. Si el `countType` usado es `sinceImagePushed`, entonces el valor es el límite de edad máximo para sus imágenes.

Action

`type`

Tipo: string.

Obligatorio: sí

Especifique un tipo de acción. El valor admitido es `expire`.

Reglas de evaluación de la política del ciclo de vida

El evaluador de políticas de ciclo de vida se encarga de analizar el código JSON en texto sin formato y de aplicarlo a las imágenes en el repositorio especificado. Cuando cree un política de ciclo de vida, debe tener en cuenta las siguientes reglas:

- Una imagen puede ser marcada para vencimiento exactamente por una o ninguna regla.
- Una imagen que cumpla los requisitos de etiquetado de una regla no puede ser marcada para vencimiento por una regla con una prioridad menor.
- Las reglas no pueden marcar nunca imágenes que están marcadas con reglas de mayor prioridad, pero puede seguir identificándolas si no han caducado.
- El conjunto de reglas debe contener un conjunto único de prefijos de etiqueta.
- Solo una regla puede seleccionar imágenes sin etiquetar.
- El vencimiento se ordena siempre por `pushed_at_time` y las imágenes más antiguas caducan siempre antes que las más nuevas.
- Al utilizar el `tagPrefixList`, una imagen se ajusta correctamente si todos de las etiquetas en el `tagPrefixList` se coincide con cualquiera de las etiquetas de la imagen.
- Con `countType = imageCountMoreThan`, las imágenes se clasifican de más jóvenes a más antiguas según `pushed_at_time` y, a continuación, todas las imágenes superiores al recuento especificado han caducado.
- Con `countType = sinceImagePushed`, todas las imágenes cuyo `pushed_at_time` es anterior al número especificado de días según `countNumber` ha caducado.

Crear una vista previa de la política del ciclo de vida

La vista preliminar de una política de ciclo de vida le permite ver el impacto de una política de ciclo de vida en un repositorio de imágenes antes de ejecutarla. En el siguiente procedimiento se muestra cómo crear una vista previa de la política de ciclo de vida.

Para crear una vista previa de una política de ciclo de vida mediante la consola

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio en el que desea obtener la vista previa de una política de ciclo de vida.
3. En el panel de navegación, seleccione Repositorios y seleccione un repositorio.
4. En el Repositorios: ***`repository_name`*** página, en el panel de navegación elegir Política del ciclo de vida.
5. En el Repositorios: ***`repository_name`***: Política del ciclo de vida página, elegir Editar reglas de prueba, , Crear regla.
6. Especifique los siguientes detalles para la regla de la política de ciclo de vida:
   a. Para Prioridad de regla, escriba un número para la prioridad de regla.
   b. Para Descripción de la regla, escriba una descripción para la regla de la política del ciclo de vida.
   c. Para Estado de imagen, elegir Etiquetado, , Sin etiquetar, o Cualquier.
   d. Si ha especificado `Tagged` para Estado de imagen, entonces para Prefijos de etiquetas, puede especificar opcionalmente una lista de etiquetas de imagen en las que tomar medidas con la política del ciclo de vida. Si ha especificado `Untagged`, este campo debe estar vacío.
   e. Para Criterios de coincidencia, elegir valores para Puesto que la imagen se ha pulsado o Recuento de imágenes más de (si procede).
7. Elegir Guardar.
8. Cree reglas de política de ciclo de vida adicionales repitiendo los pasos 5–7.
9. Para ejecutar la vista previa de la política del ciclo de vida, seleccione Guardar y ejecutar prueba.
10. Bajo Coincidencias de imagen para las reglas del ciclo de vida de la prueba, revise el impacto de la vista previa de la política del ciclo de vida.
11. Si está satisfecho con los resultados de la vista previa, elija Aplicar como política de ciclo de vida para crear una política de ciclo de vida con las reglas especificadas.

    Note

    Una vez creada una política de ciclo de vida, las imágenes a las que afecta esta política caducan al cabo de 24 horas.

Crear una política de ciclo de vida

Una política de ciclo de vida le permite crear un conjunto de reglas que marquen las imágenes del repositorio sin utilizar para vencimiento. En el siguiente procedimiento se muestra cómo crear una política de ciclo de vida. Una vez creada una política de ciclo de vida, las imágenes a las que afecta esta política caducan al cabo de 24 horas.

Para crear una política de ciclo de vidaAWS CLI)

Para crear una política de ciclo de vida utilizando el AWS CLI

1. Obtenga el ID del repositorio para el que va a crear la política de ciclo de vida:

```
aws ecr describe-repositories
```

2. Crear una política de ciclo de vida

```
aws ecr put-lifecycle-policy [--registry-id <string>] --repository-name <string> --
lifecycle-policy-text <string>
```

Para crear una política de ciclo de vidaConsola de administración de AWS)

Para crear una política de ciclo de vida mediante la consola

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región que contiene el repositorio para el que desea crear una política de ciclo de vida.
3. En el panel de navegación, seleccione Repositorios y seleccione un repositorio.
4. En el Repositorios: ***repository_name*** página, en el panel de navegación elegir Política del ciclo de vida.
5. En el Repositorios: ***repository_name***: Política del ciclo de vida página, elegir Crear regla.
6. Especifique los siguientes detalles para la regla de la política de ciclo de vida:
   a. Para Prioridad de regla, escriba un número para la prioridad de regla.
   b. Para Descripción de la regla, escriba una descripción para la regla de la política del ciclo de vida.
   c. Para Estado de imagen, elegir Etiquetado, , Sin etiquetar, o Cualquier.
   d. Si ha especificado `Tagged` para Estado de imagen, entonces para Prefijos de etiquetas, puede especificar opcionalmente una lista de etiquetas de imagen en las que tomar medidas con la política del ciclo de vida. Si ha especificado `Untagged`, este campo debe estar vacío.
   e. Para Criterios de coincidencia, elegir valores para Puesto que la imagen se ha pulsado o Recuento de imágenes más de (si procede).
7. Elegir Guardar.

Ejemplos de políticas del ciclo de vida

A continuación, se muestran políticas de ciclo de vida de ejemplo con su sintaxis.

Temas

Filtrado en la edad de la imagen

En el siguiente ejemplo se muestra la sintaxis de una política de ciclo de vida que marca para vencimiento las imágenes sin etiquetar que tienen más de `14` días:

```
{
```

```
    "rules": [
        {
            "rulePriority": 1,
            "description": "Expire images older than 14 days",
            "selection": {
                "tagStatus": "untagged",
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 14
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtrado del recuento de imágenes

En el siguiente ejemplo se muestra la sintaxis de una política de ciclo de vida que conserva solo una imagen sin etiquetar y marca para vencimiento todas las demás:

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Keep only one untagged image, expire all others",
            "selection": {
                "tagStatus": "untagged",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

Filtrado en varias reglas

El siguiente ejemplo usa varias reglas en una política de ciclo de vida. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["beta-1", "prod-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["beta-2", "prod-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["beta-3"], insertada: hace 8 días

Texto de la política de ciclo de vida:

```
{
    "rules": [
        {
            "rulePriority": 1,
```

```
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["prod"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Rule 2",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["beta"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica imágenes etiquetadas con prefijo `prod`. Debe marcar imágenes, empezando por el más antiguo, hasta que haya una o menos imágenes que coincidan. Marca la imagen A para vencimiento.
- La regla 2 identifica imágenes etiquetadas con prefijo `beta`. Debe marcar imágenes, empezando por el más antiguo, hasta que haya una o menos imágenes que coincidan. Marca la imagen A y la imagen B para vencimiento. Sin embargo, la imagen A ya ha sido identificada por la regla 1 y, si la imagen B se marcara para vencimiento, se infringiría la regla 1, por lo que se omite.
- Resultado La imagen A ha caducado.

Ejemplo B

Este es el mismo repositorio que el del ejemplo anterior, pero se ha cambiado el orden de prioridad de las reglas para ilustrar el resultado.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["beta-1", "prod-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["beta-2", "prod-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["beta-3"], insertada: hace 8 días

Texto de la política de ciclo de vida:

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["beta"],
```

```
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Rule 2",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["prod"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica imágenes etiquetadas con `beta`. Debe marcar imágenes, empezando por el más antiguo, hasta que haya una o menos imágenes que coincidan. Se identifican las tres imágenes, y la imagen A y la imagen B se marcan para vencimiento.
- La regla 2 identifica imágenes etiquetadas con `prod`. Debe marcar imágenes, empezando por el más antiguo, hasta que haya una o menos imágenes que coincidan. No se identifica ninguna imagen porque todas las imágenes disponibles ya han sido identificadas por la regla 1, por lo que no se marcan imágenes adicionales.
- Resultado Las imágenes A y B están caducadas.

Filtrado de varias etiquetas en una única regla

Los siguientes ejemplos especifican la sintaxis de la política de ciclo de vida para varios prefijos de etiqueta en una sola regla. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

Cuando se especifican varios prefijos de etiqueta en una sola regla, las imágenes deben coincidir con todos los prefijos de etiqueta especificados.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1"], insertada: hace 12 días
- Imagen B, lista de etiquetas: ["beta-1"], insertada: hace 11 días
- Imagen C, lista de etiquetas: ["alpha-2", "beta-2"], insertada: hace 10 días
- Imagen D, lista de etiquetas: ["alpha-3"], insertada: hace 4 días
- Imagen E, lista de etiquetas: ["beta-3"], insertada: hace 3 días
- Imagen F, lista de etiquetas: ["alpha-4", "beta-4"], insertada: hace 2 días

```
{
```

```
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["alpha", "beta"],
                "countType": "sinceImagePushed",
                "countNumber": 5,
                "countUnit": "days"
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica imágenes etiquetadas con `alpha` y `beta`. Ve las imágenes C y F. Debe marcar imágenes que tengan más de cinco días, que sería la imagen C.
- Resultado La imagen C ha caducado.

Ejemplo B

El ejemplo siguiente ilustra que las etiquetas no son exclusivas.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1", "beta-1", "gamma-1"], insertada: hace 10 días
- Imagen B, lista de etiquetas: ["alpha-2", "beta-2"], insertada: hace 9 días
- Imagen C, lista de etiquetas: ["alpha-3", "beta-3", "gamma-2"], insertada: hace 8 días

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["alpha", "beta"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica imágenes etiquetadas con `alpha` y `beta`. Ve todas las imágenes. Debería marcar las imágenes, empezando por la más antigua, hasta que queden una o menos imágenes. Se marcan la imagen A y la imagen B para vencimiento.
- Resultado Las imágenes A y B están caducadas.

Filtrado en todas las imágenes

Los siguientes ejemplos de políticas de ciclo de vida especifican todas las imágenes con filtros distintos. Se ofrece un repositorio de ejemplo y una política de ciclo de vida con una explicación del resultado.

Ejemplo A

A continuación, se muestra la sintaxis de una política de ciclo de vida que se aplica a todas las reglas propiedad conserva solo una imagen sin etiquetar y marca para vencimiento todas las demás.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-1"], insertada: hace 4 días
- Imagen B, lista de etiquetas: ["beta-1"], insertada: hace 3 días
- Imagen C, Etiqueta: [], Pulsado: hace 2 días
- Imagen D, lista de etiquetas: ["alpha-2"], insertada: hace 1 día

```
{
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "any",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica todas las imágenes. Detecta las imágenes A, B, C y D. Debe marcar para vencimiento todas las imágenes excepto la más reciente. Marca las imágenes A, B y C para vencimiento.
- Resultado Las imágenes A, B y C están caducadas.

Ejemplo B

El siguiente ejemplo ilustra una política de ciclo de vida que combina todos los tipos de reglas en una sola política.

Contenido del repositorio:

- Imagen A, lista de etiquetas: ["alpha-", "beta-1", "-1"], insertada: hace 4 días
- Imagen B, Etiqueta: [], Pulsado: hace 3 días
- Imagen C, lista de etiquetas: ["alpha-2"], insertada: hace 2 días
- Imagen D, lista de etiquetas: ["git hash"], insertada: hace 1 día
- Imagen E, etiqueta: [], Pulsado: hace 1 día

```
{
```

```
    "rules": [
        {
            "rulePriority": 1,
            "description": "Rule 1",
            "selection": {
                "tagStatus": "tagged",
                "tagPrefixList": ["alpha"],
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 2,
            "description": "Rule 2",
            "selection": {
                "tagStatus": "untagged",
                "countType": "sinceImagePushed",
                "countUnit": "days",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        },
        {
            "rulePriority": 3,
            "description": "Rule 3",
            "selection": {
                "tagStatus": "any",
                "countType": "imageCountMoreThan",
                "countNumber": 1
            },
            "action": {
                "type": "expire"
            }
        }
    ]
}
```

La lógica de esta política de vida sería:

- La regla 1 identifica imágenes etiquetadas con `alpha`. Identifica las imágenes A y C. Debe conservar la imagen más reciente y marcar el resto para la espiración. Marca la imagen A para vencimiento.
- La regla 2 identifica las imágenes sin etiquetar. Identifica las imágenes B y E. Debe marcar todas las imágenes anteriores a un día para vencimiento. Marca la imagen B para vencimiento.
- La regla 3 identifica todas las imágenes. Identifica las imágenes A, B, C, D y E. Debe mantener la imagen más reciente y marcar el resto para vencimiento. Sin embargo, no puede marcar las imágenes A, B, C o E porque se identificaron con reglas de mayor prioridad. Marca la imagen D para vencimiento.
- Resultado Las imágenes A, B y D están caducadas.

Mutabilidad de etiquetas de imágenes

Puede configurar un repositorio para que sea inmutable y evitar así que se sobrescriban las etiquetas de imagen. Con las etiquetas inmutables configuradas como repositorio, se devuelve un error `ImageTagAlreadyExistsException` si intenta insertar una imagen con una etiqueta que ya está en el repositorio.

Puede utilizar las herramientas Consola de administración de AWS y AWS CLI para configurar la mutabilidad de las etiquetas de imagen de un nuevo repositorio durante su creación o de un repositorio existente en cualquier momento. Para ver los pasos de la consola, consulte Creación de un repositorio (p. 25) y Edición de un repositorio (p. 28).

Para crear un repositorio con etiquetas inmutables configuradas

Utilice uno de los siguientes comandos para crear un nuevo repositorio de imágenes con etiquetas inmutables configuradas.

- create-repository (AWS CLI)

```
aws ecr create-repository --repository-name name --image-tag-mutability IMMUTABLE --
region us-east-2
```

- New-ECRRepository (Herramientas de AWS para Windows PowerShell)

```
New-ECRRepository -RepositoryName name -ImageTagMutability IMMUTABLE -Region us-east-2 -
Force
```

Para actualizar la configuración de mutabilidad de las etiquetas de imagen en un repositorio existente

Utilice uno de los siguientes comandos para actualizar la configuración de mutabilidad de las etiquetas de imagen en un repositorio existente.

- put-image-tag-mutability (AWS CLI)

```
aws ecr put-image-tag-mutability --repository-name name --image-tag-mutability IMMUTABLE
 --region us-east-2
```

- Write-ECRImageTagMutability (Herramientas de AWS para Windows PowerShell)

```
Write-ECRImageTagMutability -RepositoryName name -ImageTagMutability IMMUTABLE -
Region us-east-2 -Force
```

Escaneo de imágenes

El escaneo de imágenes de Amazon ECR de Amazon ECR ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. utiliza la base de datos de vulnerabilidades y exposiciones comunes (CVE) del proyecto Clair de código abierto y proporciona una lista de resultados de análisis. Puede revisar los resultados del escaneo para obtener información sobre la seguridad de las imágenes del contenedor que se están implementando. Para obtener más información acerca de Clair, consulte Clair en GitHub.

Amazon ECR utiliza la gravedad de CVE del origen de distribución ascendente si está disponible; de lo contrario, usamos la puntuación del Sistema de puntuación de vulnerabilidad común (CVSS). La puntuación CVSS se puede utilizar para obtener la calificación de gravedad de vulnerabilidad de NVD. Para obtener más información, consulte NVD Vulnerability Severity Ratings.

Puede escanear manualmente las imágenes de contenedor almacenadas en Amazon ECR. También puede configurar sus repositorios para escanear imágenes cuando las inserte en un repositorio. Los últimos resultados de escaneo de imagen completados se pueden recuperar para cada imagen.

Amazon ECR envía un evento a Amazon EventBridge (anteriormente llamado Eventos de CloudWatch) cuando se completa un escaneo de imagen. Para obtener más información, consulte Amazon ECR y EventBridge (p. 105).

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte Solución de problemas de escaneo de imágenes (p. 125).

Temas

Configuración de un repositorio para escaneo al insertar

Puede configurar la configuración del escaneo de imágenes para un nuevo repositorio durante la creación o para un repositorio existente. Cuando se habilita el escaneo al insertar las imágenes se escanean después de insertarlas en un repositorio. Si scan on push está deshabilitado en un repositorio, debe iniciar manualmente cada escaneo de imagen para obtener los resultados del escaneo.

Temas

Creación de un nuevo repositorio para escaneo al insertar

Cuando se configura un nuevo repositorio para escaneo al insertar, se escanearán todas las nuevas imágenes enviadas al repositorio. Los resultados del último escaneo de imagen completado se pueden recuperar. Para obtener más información, consulte Recuperación de resultados de escaneo de imágenes (p. 62).

Para ver los pasos en la Consola de administración de AWS, consulte Creación de un repositorio (p. 25).

Para crear un repositorio configurado para el escaneo al insertar (AWS CLI)

Utilice el siguiente comando para crear un nuevo repositorio con el escaneo al insertar configurado.

- create-repository (AWS CLI)

```
aws ecr create-repository --repository-name name --image-scanning-configuration
 scanOnPush=true --region us-east-2
```

Para crear un repositorio configurado para el escaneo al insertar (Herramientas de AWS para Windows PowerShell)

Utilice el siguiente comando para crear un nuevo repositorio con el escaneo al insertar configurado.

- New-ECRRepository (Herramientas de AWS para Windows PowerShell)

```
New-ECRRepository -RepositoryName name -ImageScanningConfiguration_ScanOnPush true -
Region us-east-2 -Force
```

Configurar un repositorio existente para escaneo al insertar

Los repositorios existentes se pueden configurar para escanear imágenes cuando las inserte en un repositorio. Esta configuración se aplicará a futuros envíos de imagen. Los resultados del último escaneo de imagen completado se pueden recuperar. Para obtener más información, consulte Recuperación de resultados de escaneo de imágenes (p. 62).

Para ver los pasos en la Consola de administración de AWS, consulte Edición de un repositorio (p. 28).

Para editar la configuración de un repositorio existente (AWS CLI)

Utilice el siguiente comando para editar la configuración de escaneo de imágenes de un repositorio existente.

- put-image-scanning-configuration (AWS CLI)

```
aws ecr put-image-scanning-configuration --repository-name name --image-scanning-
configuration scanOnPush=true --region us-east-2
```

> **Note**
>
> Para deshabilitar el escaneo al insertar para un repositorio, especifique `scanOnPush=false`.

Para editar la configuración de un repositorio existente (Herramientas de AWS para Windows PowerShell)

Utilice el siguiente comando para editar la configuración de escaneo de imágenes de un repositorio existente.

- New-ECRRepository (Herramientas de AWS para Windows PowerShell)

```
Write-ECRImageScanningConfiguration -RepositoryName name -
ImageScanningConfiguration_ScanOnPush true -Region us-east-2 -Force
```

Escaneo manual de una imagen

Puede iniciar el escaneo de imágenes manualmente cuando desee escanear imágenes en repositorios que no están configurados para escaneo al insertar. Una imagen solo se puede escanear una vez al día. Este límite incluye el escaneo al insertar inicial, si está activado, y cualquier escaneo manual.

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte Solución de problemas de escaneo de imágenes (p. 125).

Para comenzar el escaneo manual de una imagen (consola)

Siga los pasos siguientes para comenzar el escaneo manual de una imagen mediante la Consola de administración de AWS.

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región en la que va a crear el repositorio.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories (Repositorios), elija el repositorio del que contiene la imagen que desea escanear.

5. En la página Images (Imágenes) seleccione la imagen que desea escanear y, a continuación, elija Scan (Escanear).

Para comenzar el escaneo manual de una imagen (AWS CLI)

Utilice el siguiente comando de la AWS CLI para comenzar el escaneo manual de una imagen. Puede especificar una imagen utilizando `imageTag` o `imageDigest`, ambos se pueden obtener mediante el comando list-images de la CLI.

- start-image-scan (AWS CLI)

  En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
aws ecr start-image-scan --repository-name name --image-id imageTag=tag_name --region us-east-2
```

  En el ejemplo siguiente se utiliza un resumen de imágenes.

```
aws ecr start-image-scan --repository-name name --image-id imageDigest=sha256_hash --region us-east-2
```

Para comenzar el escaneo manual de una imagen (Herramientas de AWS para Windows PowerShell)

Utilice el siguiente comando de la Herramientas de AWS para Windows PowerShell para comenzar el escaneo manual de una imagen. Puede especificar una imagen utilizando `ImageId_ImageTag` o `ImageId_ImageDigest`, ambos se pueden obtener mediante el comando Get-ECRImage de la CLI.

- Get-ECRImageScanFinding (Herramientas de AWS para Windows PowerShell)

  En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageTag tag_name -Region us-east-2 -Force
```

  En el ejemplo siguiente se utiliza un resumen de imágenes.

```
Start-ECRImageScan -RepositoryName name -ImageId_ImageDigest sha256_hash -Region us-east-2 -Force
```

Recuperación de resultados de escaneo de imágenes

Puede recuperar los resultados del escaneo del último escaneo de imagen completado. Los resultados muestran por gravedad las vulnerabilidades de software detectadas, en función de la base de datos de Vulnerabilidades y Exposiciones Comunes (CVE).

Para obtener detalles sobre la solución de problemas comunes al escanear imágenes, consulte Solución de problemas de escaneo de imágenes (p. 125).

Para recuperar los resultados del escaneo de imágenes (consola)

Siga los pasos siguientes para recuperar los resultados del escaneo de imágenes mediante la Consola de administración de AWS.

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/repositories.
2. En la barra de navegación, seleccione la región en la que va a crear el repositorio.
3. En el panel de navegación, elija Repositories.
4. En la página Repositories (Repositorios) elija el repositorio que contiene la imagen para recuperar los resultados del escaneo.
5. En la página Images (Imágenes), en la columna Vulnerabilities (Vulnerabilidades), seleccione Details (Detalles) para la imagen para la que desea recuperar los resultados del escaneo.

Para recuperar los resultados del escaneo de imágenes (AWS CLI)

Utilice el siguiente comando de la AWS CLI para recuperar los resultados del escaneo de imágenes mediante la AWS CLI. Puede especificar una imagen utilizando `imageTag` o `imageDigest`, ambos se pueden obtener mediante el comando list-images de la CLI.

- describe-image-scan-findings (AWS CLI)

  En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
aws ecr describe-image-scan-findings --repository-name name --image-id imageTag=tag_name
 --region us-east-2
```

  En el ejemplo siguiente se utiliza un resumen de imágenes.

```
aws ecr describe-image-scan-findings --repository-name name --image-id
 imageDigest=sha256_hash --region us-east-2
```

Para recuperar los resultados del escaneo de imágenes (Herramientas de AWS para Windows PowerShell)

Utilice el siguiente comando Herramientas de AWS para Windows PowerShell para recuperar los resultados del escaneo de imágenes. Puede especificar una imagen utilizando `ImageId_ImageTag` o `ImageId_ImageDigest`, ambos se pueden obtener mediante el comando Get-ECRImage de la CLI.

- Get-ECRImageScanFinding (Herramientas de AWS para Windows PowerShell)

  En el ejemplo siguiente se utiliza una etiqueta de imagen.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageTag tag_name -Region us-east-2
```

  En el ejemplo siguiente se utiliza un resumen de imágenes.

```
Get-ECRImageScanFinding -RepositoryName name -ImageId_ImageDigest sha256_hash -Region us-
east-2
```

Formatos del manifiesto de imágenes de contenedor

Amazon ECR admite los siguientes formatos del manifiesto de imágenes de contenedor:

- Docker Image Manifest V2 Schema 1 (usado con Docker versión 1.9 y anteriores)

- Docker Image Manifest V2 Schema 2 (usado con Docker versión 1.10 y posteriores)
- Especificaciones de la iniciativa de contenedores abiertos (OCI) (versión 1.0 y posteriores)

La compatibilidad con Docker Image Manifest V2 Schema 2 ofrece la siguiente funcionalidad:

- La capacidad de utilizar varias etiquetas para una imagen singular.
- Posibilidad de almacenar imágenes de contenedores Windows. Para obtener más información, consulte Insertar imágenes de Windows en Amazon ECR en la Amazon Elastic Container Service Developer Guide.

Conversión del manifiesto de imágenes de Amazon ECR

Cuando extrae e inserta imágenes en Amazon ECR, el cliente del motor de contenedores (por ejemplo, Docker) se comunica con el registro para aceptar un formato de manifiesto que entienda tanto el cliente como el registro para usarlo con la imagen.

Cuando inserta una imagen en Amazon ECR con Docker versión 1.9 o anterior, el formato del manifiesto de imágenes se almacena como Docker Image Manifest V2 Schema 1. Cuando inserta una imagen en Amazon ECR con Docker versión 1.10 o posterior, el formato del manifiesto de imágenes se almacena como Docker Image Manifest V2 Schema 2.

Cuando extrae una imagen de Amazon ECR por etiqueta, Amazon ECR devuelve el formato del manifiesto de imágenes almacenado en el repositorio. El formato se devuelve solo si el cliente entiende dicho formato. Si el cliente no entiende el formato del manifiesto de imágenes almacenado, Amazon ECR convierte el manifiesto de imágenes en un formato que se entiende. Por ejemplo, si un cliente Docker 1.9 solicita un manifiesto de imágenes que está almacenado como Docker Image Manifest V2 Schema 2, Amazon ECR devuelve el manifiesto en el formato Docker Image Manifest V2 Schema 1. En la siguiente tabla se describen las conversiones disponibles admitidas por Amazon ECR cuando se extrae una imagen por etiqueta:

Esquema solicitado por el cliente	Insertado en ECR como V2, esquema 1	Insertado en ECR como V2, esquema 2	Insertado en ECR como OCI
V2, esquema 1	No se requiere ninguna conversión	Convertido en V2, esquema 1	Convertido en V2, esquema 1
V2, esquema 2	No hay ninguna conversión disponible; el cliente utiliza V2, esquema 1	No se requiere ninguna conversión	Convertido en V2, esquema 2
OCI	No hay ninguna conversión disponible	Convertido en OCI	No se requiere ninguna conversión

> **Important**
>
> Si extrae una imagen por resumen, no hay ninguna conversión disponible. El cliente debe entender el formato del manifiesto de imágenes almacenado en Amazon ECR. Si solicita una imagen Docker Image Manifest V2 Schema 2 por resumen en un cliente Docker 1.9 o anterior, no se puede extraer la imagen. Para obtener más información, consulte Registry compatibility en la documentación de Docker.

En este ejemplo, si solicita la misma imagen por etiqueta, Amazon ECR convierte el manifiesto de imágenes en un formato que el cliente pueda entender. La imagen se extrae correctamente.

Uso de imágenes de Amazon ECR con Amazon ECS

Puede utilizar las imágenes de contenedor alojadas en Amazon ECR en las definiciones de tareas de Amazon ECS, pero debe cumplir los siguientes requisitos previos.

- Cuando utilice el tipo de lanzamiento de EC2 para sus tareas de Amazon ECS, sus instancias de contenedor deben usar al menos la versión 1.7.0 del agente de contenedor de Amazon ECS. La última versión de la AMI optimizada para Amazon ECS admite imágenes de Amazon ECR en las definiciones de tareas. Para obtener más información, incluidos los ID de las AMI optimizadas para Amazon ECS más recientes, consulte Versiones de la AMI optimizadas para Amazon ECS en la Amazon Elastic Container Service Developer Guide.
- El rol de IAM de la instancia de contenedor de Amazon ECS (`ecsInstanceRole`) que utilice debe contener los siguientes permisos de políticas de IAM para Amazon ECR.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetAuthorizationToken"
            ],
            "Resource": "*"
        }
    ]
}
```

  Si usa la política administrada AmazonEC2ContainerServiceforEC2Role, el rol de IAM de su instancia de contenedor tiene los permisos adecuados. Para comprobar si el rol es compatible con Amazon ECR, consulte Rol de IAM de la instancia de contenedor de Amazon ECS en la Amazon Elastic Container Service Developer Guide.
- En las definiciones de tareas de Amazon ECS, asegúrese de que usa la nomenclatura `registry/repository:tag` completa para sus imágenes de Amazon ECR. Por ejemplo, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`my-web-app`*`:`*`latest`*.

  El siguiente fragmento de definición de tarea muestra la sintaxis que debería utilizar para especificar una imagen de contenedor alojada en Amazon ECR en la definición de tarea de Amazon ECS.

```
{
    "family": "task-definition-name",
    ...
    "containerDefinitions": [
        {
            "name": "container-name",
            "image": "aws_account_id.dkr.ecr.region.amazonaws.com/my-web-app:latest",
            ...
        }
    ],
    ...
```

```
}
```

Uso de imágenes de Amazon ECR con Amazon EKS

Puede usar sus imágenes de Amazon ECR con Amazon EKS, pero tiene que cumplir los siguientes requisitos previos:

- El rol de IAM de nodo de trabajo Amazon EKS (`NodeInstanceRole`) que se utiliza con los nodos de trabajo debe poseer los siguientes permisos de política de IAM para Amazon ECR.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetAuthorizationToken"
            ],
            "Resource": "*"
        }
    ]
}
```

  Note

  Si utilizó `eksctl` o las plantillas de AWS CloudFormation en la Introducción a Amazon EKS para crear el clúster y los grupos de nodos de trabajo, estos permisos de IAM se aplican al rol de IAM de nodo de trabajo de forma predeterminada.
- Al hacer referencia a una imagen desde Amazon ECR, debe usar el nombre completo `registry/repository:tag` para la imagen. Por ejemplo, *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`my-web-app`*`:`*`latest`*.

Instalación de un gráfico de timón alojado en Amazon ECR con Amazon EKS

Sus gráficos de timones alojados en Amazon ECR se puede instalar en su Amazon EKS de clústeres de. Los siguientes pasos muestran este.

Prerequisites

Antes de comenzar, asegúrese de que se han completado los siguientes pasos.

- Instale el cliente de Helm versión 3. Para obtener más información, consulte Cómo instalar el timón.
- Ha enviado un gráfico de timón a su Amazon ECR del repositorio de. Para obtener más información, consulte Inserción de un gráfico de Helm (p. 41).
- Ha configurado `kubectl` para trabajar con Amazon EKS. Para obtener más información, consulte Crear un `kubeconfig` para Amazon EKS en el Guía del usuario de Amazon EKS. Si los siguientes comandos se ejecutan correctamente para el clúster, significa que está configurado correctamente.

```
kubectl get svc
```

Instalación de un Amazon ECR de timón alojado en un Amazon EKS clúster de

1. Habilite la compatibilidad con OCI en el cliente Helm 3.

   ```
   export HELM_EXPERIMENTAL_OCI=1
   ```

2. Autenticar el cliente de Helm en el Amazon ECR del registro de que su gráfico de Helm está alojado en. Debe obtener tokens de autenticación para cada registro usado, cuya validez es de 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).

   ```
   aws ecr get-login-password \
        --region us-west-2 | helm registry login \
        --username AWS \
        --password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
   ```

3. Extraiga su gráfico de Helm a su caché local.

   ```
   helm chart pull aws_account_id.dkr.ecr.region.amazonaws.com/repository-name:mychart
   ```

4. Exporte el gráfico a un directorio local. En este ejemplo, utilizamos un directorio denominado `charts`.

   ```
   helm chart export aws_account_id.dkr.ecr.region.amazonaws.com/repository-name:mychart
    --destination ./charts
   ```

5. Instale el gráfico.

   ```
   helm install ecr-chart-demo ./mychart
   ```

   El resultado debe tener un aspecto similar a este:

   ```
   NAME: ecr-chart-demo
   LAST DEPLOYED: Wed Sep  2 14:32:07 2020
   NAMESPACE: default
   STATUS: deployed
   REVISION: 1
   NOTES:
   ```

6. Verifique la instalación del gráfico. El resultado será una representación YAML de los recursos de Kubernetes implementados por el gráfico.

   ```
   helm get manifest ecr-chart-demo
   ```

7. (Opcional) Consulte el gráfico de timones que se ejecuta en su Amazon EKS del receptáculo.

   ```
   kubectl get pods --all-namespaces
   ```

8. Cuando haya terminado, puede eliminar la versión del gráfico del clúster de.

   ```
   helm uninstall ecr-chart-demo
   ```

Imagen de contenedor Linux de Amazon

La imagen de contenedor de Amazon Linux se construye desde los mismos componentes de software que se incluyen en la AMI de Amazon Linux. Está disponible para su uso en cualquier entorno como imagen base para cargas de trabajo de Docker. Si utiliza la AMI de Amazon Linux para aplicaciones en Amazon EC2, puede incluir en contenedores las aplicaciones con la imagen de contenedor de Amazon Linux.

Puede usar la imagen de contenedor de Amazon Linux de su entorno de desarrollo local e insertar su aplicación en la nube de AWS con Amazon ECS. Para obtener más información, consulte Uso de imágenes de Amazon ECR con Amazon ECS (p. 65).

La imagen de contenedor Linux de Amazon está disponible en Amazon ECR y en Docker Hub. Puede encontrar información sobre compatibilidad con la imagen de contenedor Linux de Amazon en los foros para desarrolladores de AWS.

Para extraer la imagen del contenedor de Amazon Linux de Amazon ECR

1. Autentique su cliente de Docker en el registro de Amazon ECR de la imagen del contenedor de Amazon Linux. Los tokens de autenticación son válidos durante 12 horas. Para obtener más información, consulte Autenticación de registros privados (p. 14).

   Note

   El comando get-login-password está disponible en la AWS CLI a partir de la versión `1.17.10`. Para obtener más información, consulte Instalación de la interfaz de línea de comandos de AWS en la AWS Command Line Interface Guía del usuario.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-
   stdin 137112412989.dkr.ecr.us-east-1.amazonaws.com
   ```

   La salida es la siguiente:

   ```
   Login succeeded
   ```

   Important

   Si recibe un error, instale o actualice a la versión más reciente de la AWS CLI. Para obtener más información, consulte Instalación de la AWS Command Line Interface en la AWS Command Line Interface Guía del usuario.

2. (Opcional) Puede listar las imágenes dentro de un repositorio de Amazon Linux con el comando aws ecr list-images. La etiqueta `latest` se corresponde siempre con la última imagen del contenedor de Amazon Linux disponible.

   ```
   aws ecr list-images --region us-east-1 --registry-id 137112412989 --repository-name
    amazonlinux
   ```

3. Extraiga la imagen del contenedor de Amazon Linux con el comando docker pull.

   ```
   docker pull 137112412989.dkr.ecr.us-east-1.amazonaws.com/amazonlinux:latest
   ```

4. (Opcional) Ejecute el contenedor localmente.

   ```
   docker run -it 137112412989.dkr.ecr.us-east-1.amazonaws.com/amazonlinux:latest /bin/
   bash
   ```

Para extraer la imagen del contenedor de Amazon Linux de Docker Hub

1. Extraiga la imagen del contenedor de Amazon Linux con el comando docker pull.

```
docker pull amazonlinux
```

2. (Opcional) Ejecute el contenedor localmente.

```
docker run -it amazonlinux:latest /bin/bash
```

Seguridad en Amazon EC2 Container Registry

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y la seguridad en la nube:

- Seguridad de la nube – AWS es responsable de proteger la infraestructura que funciona AWS servicios en el AWS Nube. AWS también le ofrece servicios que puede utilizar de forma segura. Los auditores de terceros comprueban y verifican con regularidad la efectividad de nuestra seguridad como parte de la AWS programas de cumplimiento. Para conocer los programas de cumplimiento aplicables a Amazon ECR, ver AWS Servicios en el ámbito del programa de cumplimiento.
- Seguridad en la nube – Su responsabilidad está determinada por el AWS el servicio que utiliza. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayudará a conocer cómo puede aplicar el modelo de responsabilidad compartida cuando utilice Amazon ECR. En los siguientes temas, se le mostrará cómo configurar Amazon ECR para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios AWS que le ayuden a controlar y asegurar su Amazon ECR recursos.

Temas:

Identity and Access Management para Amazon EC2 Container Registry

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda a un administrador a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede ser autenticado (iniciar sesión) y estar autorizado (tener permisos) para utilizar los recursos de Amazon ECR. IAM es un servicio de AWS que se puede utilizar sin costo adicional.

Temas

Audience

La forma en la que utilice AWS Identity and Access Management (IAM) varía en función del trabajo que realice en Amazon ECR.

Usuario de servicio: si utiliza el servicio Amazon ECR para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon ECR para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en Amazon ECR, consulte Solución de problemas de identidad y acceso en Amazon EC2 Container Registry (p. 86).

Administrador de servicio: si está a cargo de los recursos de Amazon ECR en su empresa, probablemente tenga acceso completo a Amazon ECR. Su trabajo consiste en determinar qué a características y recursos de Amazon ECR deben acceder sus empleados. A continuación, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Amazon ECR, consulte Funcionamiento de Amazon EC2 Container Registry con IAM (p. 75).

Administrator de IAM: si es un administrador de IAM, es posible que quiera conocer información sobre cómo escribir políticas para administrar el acceso a Amazon ECR. Para ver ejemplos de políticas basadas en la identidad de Amazon ECR que puede utilizar en IAM, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Para obtener más información acerca de cómo iniciar sesión con la Consola de administración de AWS, consulte Iniciar sesión en la Consola de administración de AWS como usuario de IAM usuario o usuario raíz en la Guía del usuario de IAM.

Debe estar autenticado (haber iniciado sesión en AWS) como Usuario de la cuenta raíz de AWS, usuario de IAM o asumiendo un rol de IAM. También puede utilizar la autenticación de inicio de sesión único de su empresa o incluso iniciar sesión con Google o Facebook. En estos casos, su administrador habrá configurado previamente la federación de identidad mediante roles de IAM. Cuando obtiene acceso a AWS mediante credenciales de otra empresa, asume un rol indirectamente.

Para iniciar sesión directamente en la Consola de administración de AWS, use la contraseña con su dirección de correo electrónico usuario raíz o el nombre de usuario de IAM. Puede obtener acceso a AWS mediante programación utilizando sus claves de acceso de usuario usuario raíz o de IAM. AWS proporciona SDK y herramientas de línea de comandos para firmar criptográficamente su solicitud con sus credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. Para ello, utilice Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre las solicitudes de autenticación, consulte Proceso de firma de Signature Version 4 en la AWS General Reference.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor

(MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Uso de Multi-Factor Authentication (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Cuando se crea por primera vez una cuenta de AWS, se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de AWS de la cuenta de usuario raíz y se obtiene acceso a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos que no utilice usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar exclusivamente usuario raíz para crear el primer usuario de IAM. A continuación, guarde las credenciales de usuario raíz en un lugar seguro y utilícelas únicamente para algunas tareas de administración de cuentas y servicios.

Usuarios y grupos de IAM

Un usuario de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Un usuario de IAM puede tener credenciales a largo plazo, como un nombre de usuario y una contraseña o un conjunto de claves de acceso. Para obtener más información acerca de cómo generar claves de acceso, consulte Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM. Al generar claves de acceso para un usuario de IAM, asegúrese de ver y guardar de forma segura el par de claves. No puede recuperar la clave de acceso secreta en el futuro. En su lugar, debe generar un nuevo par de claves de acceso.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese Administradores de IAM y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la Consola de administración de AWS cambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Si necesita más información sobre los métodos de uso de los roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Permisos de usuario temporales de IAM: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso de usuario federado: En lugar de crear un usuario de IAM, puede utilizar identidades existentes de AWS Directory Service, del directorio de usuarios de la empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta obtenga acceso a los recursos de su cuenta. Los roles son la forma principal

de conceder acceso entre cuentas. Sin embargo, con algunos servicios de AWS, puede asociar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

- Acceso entre servicios: Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - Permisos principales: When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, Resources, and Condition Keys for Amazon EC2 Container Registry in the Service Authorization Reference.
  - Rol de servicio: Un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Los roles de servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.
  - Role vinculado al servicio: A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- Aplicaciones que se ejecutan en Amazon EC2: Puede utilizar un rol de IAM para administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y realizan solicitudes de la AWS CLI o la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la misma. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información acerca del uso de los roles de IAM o usuarios de IAM, consulte Cuándo crear un rol de IAM (en vez de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se asocian a identidades de IAM o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. Puede iniciar sesión como usuario usuario raíz o IAM o puede asumir un rol de IAM. Cuando realiza una solicitud, AWS evalúa las políticas relacionadas basadas en identidades o en recursos. Los permisos en las políticas determinan si la solicitud se permite o se deniega. Las mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información acerca de la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas de JSON en la Guía del usuario de IAM.

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

Cada entidad de IAM (usuario o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe asociarle una política de permisos. O bien el administrador puede añadir al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la Consola de administración de AWS, la AWS CLI o la API de AWS.

Políticas basadas en la identidad

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the Guía del usuario de IAM.

Las políticas basadas en identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM role trust policies and Amazon S3 bucket policies. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Las políticas basadas en recursos son políticas en línea que se encuentran en ese servicio. No puede utilizar políticas administradas por AWS de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite otros tipos de políticas menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite definir los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidades de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información acerca de los límites de permisos, consulte see Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de forma centralizada varias cuentas de AWS que posee su negocio. Si habilita todas las funciones en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario de la cuenta raíz de AWS. Para obtener más información acerca de Organizaciones y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las

políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS determina si permitir una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Funcionamiento de Amazon EC2 Container Registry con IAM

Antes de utilizar IAM para administrar el acceso a Amazon ECR, debe saber qué características de IAM están disponibles para utilizarse con Amazon ECR. Para obtener una perspectiva general de cómo Amazon ECR y otros servicios de AWS funcionan con IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Temas

Políticas basadas en identidades de Amazon ECR

Con las políticas basadas en identidad de IAM, puede especificar las acciones permitidas o denegadas y los recursos además de las condiciones en las que se permiten o deniegan las acciones. Amazon ECR admite acciones, recursos y claves de condiciones específicos. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso a una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para otorgar permisos para realizar la operación asociada.

Las acciones de políticas de Amazon ECR utilizan el siguiente prefijo antes de la acción: `ecr:`: . Por ejemplo, para conceder a alguien permiso para crear un repositorio de Amazon ECR con la operación de la API Amazon ECR `CreateRepository` de `ecr:CreateRepository`, incluya la acción en su política. Las instrucciones de política deben incluir un elemento `Action` o `NotAction`. Amazon ECR define su propio conjunto de acciones, que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "ecr:action1",
      "ecr:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen por la palabra `Describe`, incluya la siguiente acción:

```
"Action": "ecr:Describe*"
```

Para ver una lista de acciones de Amazon ECR, consulte Acciones, recursos y claves de condición de Amazon EC2 Container Registry en la Guía del usuario de IAM.

Resources

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Una práctica recomendada consiste en especificar un recurso utilizando su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Un recurso de repositorio de Amazon ECR tiene el siguiente ARN:

```
arn:${Partition}:ecr:${Region}:${Account}:repository/${Repository-name}
```

Para obtener más información sobre el formato de ARNs, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Por ejemplo, para especificar el repositorio `my-repo` en la región `us-east-1` en la instrucción, utilice el siguiente ARN:

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
```

Para especificar todos los repositorios que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:ecr:us-east-1:123456789012:repository/*"
```

Para especificar varios recursos en una única instrucción, separe el ARNs con comas.

```
"Resource": [
      "resource1",
      "resource2"
```

Para ver una lista de tipos de recursos de Amazon ECR y sus ARNs, consulte Recursos definidos por Amazon EC2 Container Registry en la Guía del usuario de IAM. Para obtener información sobre las

acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por Amazon EC2 Container Registry.

Claves de condición

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que coincida la condición de la política con valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Amazon ECR define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

La mayoría de las acciones de Amazon ECR admiten las claves de condición `aws:ResourceTag` y `ecr:ResourceTag`. Para obtener más información, consulte Uso del control de acceso basado en etiquetas (p. 85).

Para ver una lista de claves de condición de Amazon ECR, consulte Claves de condición definidas por Amazon EC2 Container Registry en la Guía del usuario de IAM. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon EC2 Container Registry.

Examples

Para ver ejemplos de políticas de Amazon ECR basadas en identidades, consulte Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades (p. 82).

Políticas basadas en recursos de Amazon ECR

Las políticas basadas en recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso Amazon ECR y en qué condiciones. Amazon ECR admite políticas de permisos basadas en recursos para repositorios de Amazon ECR. Las políticas basadas en recursos le permiten conceder a otras cuentas permisos de uso para cada recurso. También puede utilizar una política basada en recursos para permitir a un servicio de AWS acceder a los repositorios de Amazon ECR.

Para hacer posible el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de la política basada en recursos. Añadir a una política basada en recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de

confianza. Cuando el principal y el recurso se encuentran en cuentas de AWS diferentes, también debe conceder a la entidad principal permiso para obtener acceso al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

El servicio Amazon ECR solo admite un tipo de política basada en recursos denominada política de repositorios, que se asocia a un repositorio. Esta política indica las entidades principales (cuentas, usuarios, roles y usuarios federados) que pueden realizar acciones en el repositorio.

Para obtener información sobre cómo asociar una política basada en recursos a un repositorio, consulte Políticas de repositorio (p. 29).

Examples

Para ver ejemplos de políticas basadas en recursos de Amazon ECR, consulte Ejemplos de políticas de repositorio (p. 31).

Autorización basada en etiquetas de Amazon ECR

Puede adjuntar etiquetas a los recursos de Amazon ECR o transferirlas en una solicitud a Amazon ECR. Para controlar el acceso según las etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política mediante las claves de condición `ecr:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Para obtener más información acerca del etiquetado de recursos de Amazon ECR, consulte Etiquetado de un repositorio deAmazon ECR (p. 35).

Para ver un ejemplo de política basada en la identidad para limitar el acceso a un recurso basado en las etiquetas de dicho recurso, consulte Uso del control de acceso basado en etiquetas (p. 85).

Roles de IAM para Amazon ECR

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con Amazon ECR

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de la API de AWS STS, como AssumeRole o GetFederationToken.

Amazon ECR admite el uso de credenciales temporales.

Roles vinculados a servicios

Los roles vinculados a servicios permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon ECR no admite roles vinculados a servicios.

Políticas administradas de Amazon ECR

Amazon ECR proporciona varias políticas administradas que se pueden asociar a usuarios de IAM o a instancias de EC2 para permitir diferentes niveles de control sobre los recursos y las operaciones de la API de Amazon ECR. Puede aplicar estas políticas directamente o puede usarlas como punto de partida para

crear las suyas propias. Para obtener más información acerca de cada una de las operaciones de la API mencionadas en estas políticas, consulte el tema sobre acciones en la Amazon EC2 Container Registry API Reference.

Temas

- AmazonEC2ContainerRegistryFullAccess (p. 79)
- AmazonEC2ContainerRegistryPowerUser (p. 79)
- AmazonEC2ContainerRegistryReadOnly (p. 80)

AmazonEC2ContainerRegistryFullAccess

Esta política administrada es un punto de partida para los clientes que buscan proporcionar a un usuario o rol de IAM acceso de administrador completo para administrar su uso de Amazon ECR. La función Políticas de ciclo de vida de Amazon ECR permite a los clientes especificar la administración del ciclo de vida de las imágenes en un repositorio. Los eventos de política de ciclo de vida se notifican como eventos de CloudTrail y Amazon ECR se integra con AWS CloudTrail para mostrar los eventos de política de ciclo de vida de un cliente directamente en la consola de Amazon ECR. La política de IAM administrada `AmazonEC2ContainerRegistryFullAccess` incluye el permiso `cloudtrail:LookupEvents` para facilitar este comportamiento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:*"
      ],
      "Resource": "*"
    }
  ]
}
```

AmazonEC2ContainerRegistryPowerUser

Esta política administrada proporciona a los usuarios avanzados acceso a Amazon ECR para leer y escribir en los repositorios, pero no permite eliminar los repositorios ni cambiar los documentos de política aplicados a ellos.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "ecr:GetAuthorizationToken",
   "ecr:BatchCheckLayerAvailability",
   "ecr:GetDownloadUrlForLayer",
   "ecr:GetRepositoryPolicy",
   "ecr:DescribeRepositories",
   "ecr:ListImages",
   "ecr:DescribeImages",
   "ecr:BatchGetImage",
   "ecr:InitiateLayerUpload",
   "ecr:UploadLayerPart",
   "ecr:CompleteLayerUpload",
   "ecr:PutImage"
  ],
  "Resource": "*"
```

```
 }]
}
```

AmazonEC2ContainerRegistryReadOnly

Esta política administrada proporciona acceso de solo lectura a Amazon ECR, como la posibilidad de mostrar repositorios y las imágenes incluidas en estos y extraer imágenes de Amazon ECR con la CLI de Docker.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "ecr:GetAuthorizationToken",
   "ecr:BatchCheckLayerAvailability",
   "ecr:GetDownloadUrlForLayer",
   "ecr:GetRepositoryPolicy",
   "ecr:DescribeRepositories",
   "ecr:ListImages",
   "ecr:DescribeImages",
   "ecr:BatchGetImage"
  ],
  "Resource": "*"
 }]
}
```

Uso de roles vinculados a servicios de Amazon ECR

Amazon EC2 Container Registry (Amazon ECR) utiliza AWS Identity and Access Managementroles vinculados a servicios de IAM () para proporcionar acceso para replicar recursos. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon ECR. El rol vinculado al servicio está predefinido por Amazon ECR. Incluye todos los permisos que el servicio requiere para admitir la replicación de imágenes entre regiones y entre cuentas de su registro. Después de configurar la replicación para su registro, se crea automáticamente un rol vinculado al servicio de en su nombre. Para obtener más información, consulte Configuración de replicación (p. 17).

Con un rol vinculado a un servicio, resulta más sencillo configurar la replicación con Amazon ECR. El motivo es que, al utilizarlo, no tiene que añadir manualmente todos los permisos necesarios. Amazon ECR define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon ECR puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos. La política de permisos no se puede asociar a ninguna otra entidad de IAM.

El rol vinculado al servicio solo se puede eliminar después de deshabilitar la replicación en el registro. Esto garantiza que no elimine accidentalmente el permiso para que Amazon ECR replique sus imágenes.

Para obtener información sobre otros servicios que admiten los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. En esta página vinculada, busque los servicios con la opción Yes (Sí) en la columna Service-linked role (Rol vinculado a servicio). Seleccione una opción Yes (Sí) con un enlace para ver la documentación pertinente del rol vinculado a ese servicio.

Permisos de roles vinculados a servicios de Amazon ECR

Amazon ECR usa la función vinculada al servicio denominada AWSServiceRoleForECRReplication – Allows Amazon ECR to replicate images across multiple accounts..

El rol vinculado al servicio AWSServiceRoleForECRReplication confía en los siguientes servicios para asumir el rol:

- `replication.ecr.amazonaws.com`

La política de permisos del rol permite que Amazon ECR utilice las siguientes acciones en los recursos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:CreateRepository",
                "ecr:ReplicateImage"
            ],
            "Resource": "*"
        }
    ]
}
```

Note

La `ReplicateImage` es una API interna que Amazon ECR utiliza para la replicación y no se puede llamar directamente.

Debe configurar permisos para permitir a una entidad de IAM (por ejemplo, un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a un servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon ECR

No necesita crear manualmente el rol vinculado al servicio Amazon ECR. A la hora de configurar los ajustes de replicación del registro en la Consola de administración de AWS, la AWS CLI o la API de AWS, Amazon ECR crea el rol vinculado al servicio.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al configurar los ajustes de replicación del registro, Amazon ECR vuelve a crear automáticamente el rol vinculado al servicio.

Editar un rol vinculado a un servicio para Amazon ECR

Amazon ECR no permite editar manualmente el rol vinculado a servicio AWSServiceRoleForECRReplication. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminación del rol vinculado al servicio paraAmazon ECR

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe eliminar la configuración de replicación de su registro en cada región de antes de poder eliminar manualmente el rol vinculado al servicio.

Note

Si intenta eliminar recursos mientras el servicio Amazon ECR sigue utilizando los roles, la acción de eliminación podría producir un error. Si eso sucede, espere unos minutos e inténtelo de nuevo.

Para eliminar los recursos de Amazon ECR que se utilizan en AWSServiceRoleForECRReplication

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En la barra de navegación, elija la región en la que se ha establecido la configuración de replicación.
3. En el panel de navegación, elija Registry settings (Configuración del registro).
4. Seleccione la configuración Cross-Region replication (Replicación entre regiones) y Cross-account replication (Replicación entre cuentas).
5. Seleccione Save.

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForECRReplication. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de Amazon ECR

Amazon ECR admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte AWS Regions and Endpoints.

Ejemplos de políticas de Amazon EC2 Container Registry basadas en identidades

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear ni modificar los recursos de Amazon ECR. Tampoco pueden realizar tareas mediante la Consola de administración de AWS, la AWS CLI, o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesitan esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de Amazon ECR de su cuenta. Estas acciones pueden generar costes adicionales para su cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Introducción sobre el uso de políticas administradas de AWS: para comenzar a utilizar Amazon ECR rápidamente, utilice las políticas administradas de AWS para proporcionar a los empleados los permisos

necesarios. Estas políticas ya están disponibles en su cuenta y las mantiene y actualiza AWS. Para obtener más información, consulte Introducción al uso de permisos con políticas administradas de AWS en la Guía del usuario de IAM.

- Conceder privilegios mínimos – Al crear políticas personalizadas, conceda solo los permisos necesarios para llevar a cabo una tarea. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos que son demasiado tolerantes e intentar hacerlos más severos más adelante. Para obtener más información, consulte la sección Otorgar privilegios mínimos en la Guía del usuario de IAM.
- Habilitar MFA para operaciones confidenciales – Para mayor seguridad, obligue a los usuarios de IAM a que utilicen la autenticación multifactor (MFA) para acceder a recursos u operaciones de API confidenciales. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.
- Utilizar condiciones de política para mayor seguridad – En la medida en que sea práctico, defina las condiciones en las que sus políticas basadas en identidad permitan el acceso a un recurso. Por ejemplo, puede escribir condiciones para especificar un rango de direcciones IP permitidas desde el que debe proceder una solicitud. También puede escribir condiciones para permitir solicitudes solo en un intervalo de hora o fecha especificado o para solicitar el uso de SSL o MFA. Para obtener más información, consulteElementos de la política de JSON de IAM: condición en la Guía del usuario de IAM.

Uso de la consola de Amazon ECR

Para acceder a la consola de Amazon EC2 Container Registry, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon ECR de su cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para asegurarse de que esas entidades puedan seguir utilizando la consola de Amazon ECR, asocie también una política administrada de AWS `AmazonEC2ContainerRegistryReadOnly` a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "ecr:GetAuthorizationToken",
   "ecr:BatchCheckLayerAvailability",
   "ecr:GetDownloadUrlForLayer",
   "ecr:GetRepositoryPolicy",
   "ecr:DescribeRepositories",
   "ecr:ListImages",
   "ecr:DescribeImages",
   "ecr:BatchGetImage"
  ],
  "Resource": "*"
 }]
}
```

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios ver sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye

permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso a un repositorio de Amazon ECR

En este ejemplo, desea conceder acceso a un usuario de IAM de su cuenta de AWS a uno de sus repositorios de Amazon ECR, `my-repo`. También desea permitir al usuario insertar, extraer y enumerar imágenes.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListImagesInRepository",
         "Effect":"Allow",
         "Action":[
            "ecr:ListImages"
         ],
         "Resource":"arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
      },
      {
         "Sid":"GetAuthorizationToken",
         "Effect":"Allow",
         "Action":[
            "ecr:GetAuthorizationToken"
         ],
         "Resource":"*"
      },
      {
         "Sid":"ManageRepositoryContents",
```

```
        "Effect":"Allow",
        "Action":[
               "ecr:BatchCheckLayerAvailability",
               "ecr:GetDownloadUrlForLayer",
               "ecr:GetRepositoryPolicy",
               "ecr:DescribeRepositories",
               "ecr:ListImages",
               "ecr:DescribeImages",
               "ecr:BatchGetImage",
               "ecr:InitiateLayerUpload",
               "ecr:UploadLayerPart",
               "ecr:CompleteLayerUpload",
               "ecr:PutImage"
        ],
        "Resource":"arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
     }
  ]
}
```

Uso del control de acceso basado en etiquetas

La acción de la API CreateRepository de Amazon ECR le permite especificar etiquetas al crear el repositorio. Para obtener más información, consulte Etiquetado de un repositorio deAmazon ECR (p. 35).

Para que los usuarios puedan etiquetar repositorios durante la creación, es preciso que tengan permisos para utilizar la acción que crea el recurso (por ejemplo, `ecr:CreateRepository`). Si se especifican etiquetas en la acción de creación de recursos, Amazon realiza una autorización adicional en la acción `ecr:CreateRepository` para verificar que los usuarios tengan permisos para crear etiquetas.

Puede utilizar el control de acceso basado en etiquetas mediante las políticas de IAM. A continuación se muestran algunos ejemplos.

La siguiente política solo permitiría a un usuario de IAM crear o etiquetar un repositorio como `key=environment,value=dev`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedRepository",
            "Effect": "Allow",
            "Action": [
                "ecr:CreateRepository"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "dev"
                }
            }
        },
        {
            "Sid": "AllowTagRepository",
            "Effect": "Allow",
            "Action": [
                "ecr:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "dev"
                }
```

```
            }
        }
    ]
}
```

La siguiente política permitiría a un usuario de IAM obtener acceso a todos los repositorios a menos que estuvieran etiquetados como `key=environment,value=prod`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecr:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ecr:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecr:ResourceTag/environment": "prod"
                }
            }
        }
    ]
}
```

Solución de problemas de identidad y acceso en Amazon EC2 Container Registry

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando se trabaja con Amazon ECR e IAM.

Temas

No tengo autorización para realizar una acción en Amazon ECR

Si la Consola de administración de AWS le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

En el siguiente ejemplo, el error se produce cuando el usuario `mateojackson` de IAM, intenta utilizar la consola para ver detalles sobre un repositorio, pero no tiene permisos `ecr:DescribeRepositories`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ecr:DescribeRepositories on resource: my-repo
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `my-repo` mediante la acción `ecr:DescribeRepositories`.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no está autorizado para llevar a cabo la acción `iam:PassRole`, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña. Pida a la persona que actualice sus políticas de forma que pueda transferir un rol a Amazon ECR.

Algunos servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon ECR. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

En este caso, Mary pide a su administrador que actualice sus políticas para que pueda realizar la acción `iam:PassRole`.

Quiero ver mis claves de acceso

Después de crear sus claves de acceso de usuario de IAM, puede ver su ID de clave de acceso en cualquier momento. Sin embargo, no puede volver a ver su clave de acceso secreta. Si pierde la clave de acceso secreta, debe crear un nuevo par de claves de acceso.

Las claves de acceso se componen de dos partes: un ID de clave de acceso (por ejemplo, `AKIAIOSFODNN7EXAMPLE`) y una clave de acceso secreta (por ejemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). El ID de clave de acceso y la clave de acceso secreta se utilizan juntos, como un nombre de usuario y contraseña, para autenticar sus solicitudes. Administre sus claves de acceso con el mismo nivel de seguridad que para el nombre de usuario y la contraseña.

> **Important**
>
> No proporcione las claves de acceso a terceras personas, ni siquiera para que le ayuden a buscar el ID de usuario canónico. Si lo hace, podría conceder a otra persona acceso permanente a su cuenta.

Cuando cree un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe añadir nuevas claves de acceso a su usuario de IAM. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear uno nuevo. Para ver las instrucciones, consulte Administración de las claves de acceso en la Guía del usuario de IAM.

Soy administrador y deseo permitir que otros obtengan acceso a Amazon ECR

Para permitir que otros obtengan acceso a Amazon ECR, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para obtener acceso a AWS. A continuación, debe asociar una política a la entidad que le conceda los permisos correctos en Amazon ECR.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir a personas externas a mi cuenta de AWS el acceso a mis recursos de Amazon ECR

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Amazon ECR admite estas características, consulte Funcionamiento de Amazon EC2 Container Registry con IAM (p. 75).
- Para aprender cómo proporcionar acceso a sus recursos en cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo ofrecer acceso a sus recursos a cuentas de AWS de terceros, consulte Proporcionar acceso a las cuentas de AWS propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información acerca de cómo ofrecer acceso a la identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca de la diferencia entre utilizar los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Protección de datos en Amazon ECR

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Elastic Container Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de AWS que utiliza. Para obtener más información acerca de la privacidad de datos, consulte las Preguntas frecuentes sobre privacidad de datos. Para obtener más información sobre la protección de datos en Europa, consulte la publicación de blog AWS Shared Responsibility Model and GDPR en el blog de seguridad de AWS.

Para fines de protección de datos, recomendamos proteger las credenciales de cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera,solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También le recomendamos proteger sus datos de las siguientes formas:

- Utilice la autenticación multifactor (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Le recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice los servicios de seguridad administrados avanzados como, por ejemplo, Amazon Macie, que ayudan a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información acerca

de los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Name (Nombre). No debe introducir esta información cuando trabaje con Amazon ECS u otros servicios de AWS a través de la consola, la API, la AWS CLI de AWS o los SDK de AWS. Cualquier dato que escriba en Amazon ECS o en otros servicios se puede incluir en los registros de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Temas

Cifrado en reposo

Amazon ECR almacena imágenes en buckets de Amazon S3 que Amazon ECR administra. De forma predeterminada, Amazon ECR utiliza el cifrado en el servidor con claves de cifrado administradas por Amazon S3 que cifran los datos en reposo mediante un algoritmo de cifrado AES-256. Esto no requiere ninguna acción por su parte y se ofrece sin cargo adicional. Para obtener más información, consulte Protección de los datos con el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) en la Guía para desarrolladores de Amazon Simple Storage Service.

Para tener más control sobre el cifrado de los repositorios de Amazon ECR, puede utilizar el cifrado del lado del servidor con claves maestras del cliente (CMK) almacenadas en AWS Key Management Service (AWS KMS). Al utilizar AWS KMS para cifrar los datos, puede utilizar la CMK administrada por AWS predeterminada, que se administra mediante Amazon ECR, o especificar su propia CMK (esto se denomina CMK administrada por el cliente). Para obtener más información, consulte Protección de datos con el cifrado del lado del servidor con CMKs almacenado en AWS Key Management Service (SSE-KMS) en la Guía para desarrolladores de Amazon Simple Storage Service.

Cada repositorio de Amazon ECR tiene una configuración de cifrado, que se establece al crear el repositorio. Puede utilizar diferentes configuraciones de cifrado en cada repositorio. Para obtener más información, consulte Creación de un repositorio (p. 25).

Al crear un repositorio con el cifrado de AWS KMS habilitado, se utiliza una CMK para cifrar el contenido del repositorio. Además, Amazon ECR añade una concesión AWS KMS a la CMK con el repositorio de Amazon ECR como la entidad principal beneficiaria.

Lo siguiente proporciona información general sobre cómo Amazon ECR se integra con AWS KMS para cifrar y descifrar los repositorios:

1. Al crear un repositorio, Amazon ECR envía una llamada DescribeKey a AWS KMS para validar y recuperar el nombre de recurso de Amazon (ARN) de la CMK especificada en la configuración de cifrado.
2. Amazon ECR envía dos solicitudes CreateGrant a AWS KMS para crear concesiones en la CMK para permitir a Amazon ECR cifrar y descifrar datos mediante la clave de datos.
3. Al insertar una imagen, se realiza una solicitud GenerateDataKey a AWS KMS que especifica la CMK que se debe utilizar para cifrar la capa de imagen y el manifiesto.
4. AWS KMS genera una nueva clave de datos, la cifra según la CMK especificada y envía la clave de datos cifrada para que se almacene con los metadatos de la capa de imagen y el manifiesto de la imagen.
5. Al extraer una imagen, se realiza una solicitud Decrypt a AWS KMS, especificando la clave de datos cifrada.
6. AWS KMS descifra la clave de datos cifrada y envía la clave de datos descifrada a Amazon S3.

7. La clave de datos en utilizada para descifrar la capa de imagen antes de que se extraiga la capa de imagen.
8. Al eliminar un repositorio, Amazon ECR envía dos solicitudes RetireGrant a AWS KMS para retirar las concesiones creadas para el repositorio.

Considerations

Se deben tener en cuenta los siguientes puntos al utilizar el cifrado AWS KMS con Amazon ECR.

- Si crea su repositorio de Amazon ECR con cifrado KMS y no especifica una CMK, Amazon ECR utiliza una CMK administrada por AWS con el alias `aws/ecr` de forma predeterminada. Esta CMK se crea en su cuenta la primera vez que crea un repositorio con el cifrado KMS habilitado.
- Al utilizar el cifrado de KMS con su propia CMK, la clave debe existir en la misma región que su repositorio.
- AWS KMS aplica un límite de 500 concesiones por CMK. Como resultado, existe un límite de 500 repositorios de Amazon ECR que se pueden cifrar por CMK.
- Las concesiones que Amazon ECR crea en su nombre no deben revocarse. Si revoca la concesión que concede a Amazon ECR permiso para utilizar las claves de AWS KMS de su cuenta, Amazon ECR no podrá obtener acceso a estos datos, cifrar las imágenes nuevas enviadas al repositorio ni descifrarlas cuando se extraigan. Cuando se revoca una concesión para Amazon ECR, el cambio se produce inmediatamente. Para revocar los derechos de acceso, debe eliminar el repositorio en lugar de revocar la concesión. Al eliminar un repositorio, Amazon ECR retira las concesiones en su nombre.
- El uso de claves de AWS KMS tiene un costo asociado. Para obtener más información, consulte Precios de AWS Key Management Service.

Permisos de IAM necesarios

A la hora de crear o eliminar un repositorio de Amazon ECR con cifrado del lado del servidor mediante AWS KMS, los permisos necesarios dependen de la clave maestra de cliente (CMK) específica que utilice.

Permisos de IAM necesarios al usar la CMK administrada por AWS para Amazon ECR

De forma predeterminada, cuando el cifrado de AWS KMS está habilitado para un repositorio de Amazon ECR pero no se especifica ninguna CMK, se utiliza la CMK administrada por AWS para Amazon ECR. Cuando se utiliza la CMK administrada por AWS para Amazon ECR para cifrar un repositorio, cualquier entidad principal que tenga permiso para crear un repositorio también puede habilitar el cifrado de AWS KMS en el repositorio. Sin embargo, la entidad principal de IAM que elimina el repositorio debe tener el permiso `kms:RetireGrant`. Esto permite retirar las concesiones que se añadieron a la clave AWS KMS cuando se creó el repositorio.

El siguiente ejemplo de política de IAM se puede añadir como política insertada a un usuario para garantizar que tenga los permisos mínimos necesarios para eliminar un repositorio que tenga habilitado el cifrado. La clave de AWS KMS utilizada para cifrar el repositorio se puede especificar mediante el parámetro de recurso.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-kms-permissions",
    "Statement": [
        {
            "Sid": "Allow access to retire the grants associated with the key",
            "Effect": "Allow",
            "Action": [
                "kms:RetireGrant"
```

```
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
        }
    ]
}
```

Permisos de IAM necesarios cuando se utiliza una CMK administrada por el cliente

Al crear un repositorio con el cifrado de AWS KMS habilitado mediante una CMK administrada por el cliente, existen permisos necesarios tanto para la política de claves de CMK como para la política de IAM para el usuario o rol que crea el repositorio.

Al crear su propia CMK, puede utilizar la política de claves predeterminada que AWS KMS crea o puede especificar la suya propia. Para garantizar que la CMK administrada por el cliente siga siendo administrable por el propietario de la cuenta, la política de claves de la CMK debe permitir todas las acciones de AWS KMS para el usuario raíz de la cuenta. Se pueden añadir permisos con ámbito adicionales a la política de claves, pero como mínimo se debe dar al usuario raíz permisos para administrar la CMK. Para permitir que la CMK solo se pueda utilizar para las solicitudes que se originan en Amazon ECR, puede usar la clave de condición kms:ViaService con el valor `ecr.<region>.amazonaws.com`.

La siguiente política de claves de ejemplo concede a la cuenta de AWS (usuario raíz) propietaria de la CMK acceso completo a la CMK. Para obtener más información acerca de esta política de claves de ejemplo, consulte Permite el acceso a la cuenta de AWS y habilita las políticas de IAM en la AWS Key Management Service Developer Guide.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-key-policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

El usuario de IAM, el rol de IAM o la cuenta de AWS que crea los repositorios deben tener los permisos `kms:CreateGrant`, `kms:RetireGrant` y `kms:DescribeKey`, además de los permisos de Amazon ECR necesarios.

> **Note**
>
> El permiso `kms:RetireGrant` debe añadirse a la política de IAM del usuario o rol que crea el repositorio. Los permisos `kms:CreateGrant` y `kms:DescribeKey` se pueden añadir a la política de claves para la CMK o a la política de IAM del usuario o rol que crea el repositorio. Para obtener más información sobre cómo funcionan los permisos de AWS KMS, consulte Permisos de la API de AWS KMS: : referencia de acciones y recursos en la AWS Key Management Service Developer Guide.

El siguiente ejemplo de política de IAM se puede añadir como política insertada a un usuario para garantizar que tenga los permisos mínimos necesarios para crear un repositorio con cifrado habilitado y eliminar el repositorio cuando haya terminado con él. La clave de AWS KMS utilizada para cifrar el repositorio se puede especificar mediante el parámetro de recurso.

```
{
    "Version": "2012-10-17",
    "Id": "ecr-kms-permissions",
    "Statement": [
        {
            "Sid": "Allow access to create and retire the grants associated with the key as
 well as describe the key",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/b8d9ae76-080c-4043-92EXAMPLE"
        }
    ]
}
```

Para permitir que un usuario obtenga una lista de CMKs en la consola al crear un repositorio

Al utilizar la consola de Amazon ECR para crear un repositorio, puede conceder permisos para permitir que un usuario muestre la CMKs administrada por el cliente en la región al habilitar el cifrado para el repositorio. El siguiente ejemplo de política de IAM muestra los permisos necesarios para enumerar sus CMKs y alias cuando se utiliza la consola.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}
```

Monitorear la interacción de Amazon ECR con AWS KMS

Puede utilizar AWS CloudTrail para realizar un seguimiento de las solicitudes que Amazon ECR envía a AWS KMS en su nombre. Las entradas de registro del registro de CloudTrail contienen una clave de contexto de cifrado para que se puedan identificar más fácilmente.

Contexto de cifrado de Amazon ECR

Un contexto de cifrado es un conjunto de pares de clave-valor que contiene datos no secretos arbitrarios. Cuando se incluye un contexto de cifrado en una solicitud para cifrar datos, AWS KMS vincula criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

En sus solicitudes GenerateDataKey y Decrypt a AWS KMS, Amazon ECR utiliza un contexto de cifrado con dos pares de nombre–valor que identifican el repositorio y el bucket de Amazon S3 que se están utilizando. Esto se muestra en el siguiente ejemplo. Los nombres no varían, pero los valores de contexto de cifrado combinado serán diferentes para cada valor.

```
"encryptionContext": {
```

```
    "aws:s3:arn": "arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-
ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df",
    "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
}
```

Puede utilizar el contexto de cifrado para identificar esta operación criptográfica en los registros de auditoría, como AWS CloudTrail y Amazon CloudWatch Logs, y como una condición para la autorización de las políticas y concesiones.

El contexto de cifrado de Amazon ECR se compone de dos pares de nombre-valor.

- aws:s3:arn – el primer par de nombre–valor identifica el bucket. La clave es `aws:s3:arn`. El valor es el nombre de recurso de Amazon (ARN) del bucket de Amazon S3.

  ```
  "aws:s3:arn": "ARN of an Amazon S3 bucket"
  ```

  Por ejemplo, si el ARN del bucket es `arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df`, el contexto de cifrado incluiría el siguiente par.

  ```
  "arn:aws:s3:::us-west-2-starport-manifest-bucket/EXAMPLE1-90ab-cdef-fedc-ba987BUCKET1/
  sha256:a7766145a775d39e53a713c75b6fd6d318740e70327aaa3ed5d09e0ef33fc3df"
  ```

- aws:ecr:arn – el segundo nombre–par de valores identifica el nombre de recurso de Amazon (ARN) del repositorio. La clave es `aws:ecr:arn`. El valor es el ARN del repositorio.

  ```
  "aws:ecr:arn": "ARN of an Amazon ECR repository"
  ```

  Por ejemplo, si el ARN del repositorio es `arn:aws:ecr:us-west-2:111122223333:repository/repository-name`, el contexto de cifrado incluiría el siguiente par.

  ```
  "aws:ecr:arn": "arn:aws:ecr:us-west-2:111122223333:repository/repository-name"
  ```

Troubleshooting

Al eliminar un repositorio de Amazon ECR con la consola, si el repositorio se elimina correctamente, pero Amazon ECR no puede retirar las concesiones añadidas a su CMK para su repositorio, recibirá el siguiente error.

```
The repository [{repository-name}] has been deleted successfully but the grants created by
 the kmsKey [{kms_key}] failed to be retired
```

Cuando esto suceda, puede retirar las concesiones de AWS KMS para el repositorio usted mismo.

Para retirar concesiones de AWS KMS de un repositorio manualmente

1. Enumere las concesiones para la clave de AWS KMS utilizada para el repositorio. El valor `key-id` se incluye en el error que recibe de la consola de . También puede utilizar el comando `list-keys` para mostrar la CMKs administrada por AWS y la CMKs administrada por el cliente de una región específica de su cuenta.

   ```
   aws kms list-grants \
        --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc
   ```

```
    --region us-west-2
```

El resultado incluye un `EncryptionContextSubset` con el nombre de recurso de Amazon (ARN) de su repositorio. Se puede utilizar para determinar qué concesión añadida a la clave es la que desea retirar. El valor `GrantId` se utilizará al retirar la concesión en el siguiente paso.

2. Retire cada concesión para la clave AWS KMS añadida al repositorio. Reemplace el valor de *`GrantId`* con el ID de la concesión de la salida del paso anterior.

```
aws kms retire-grant \
    --key-id b8d9ae76-080c-4043-9237-c815bfc21dfc \
    --grant-id GrantId \
    --region us-west-2
```

Validación de la conformidad para Amazon EC2 Container Registry

Auditores externos evalúan la seguridad y la conformidad de Amazon EC2 Container Registry en distintos programas de conformidad de AWS. Esto incluye SOC, PCI, HIPAA y otros.

Para obtener una lista de servicios de AWS en el ámbito de programas de cumplimiento específicos, consulte Servicios de AWS en el ámbito del programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Amazon ECR se determina en función de la confidencialidad de los datos, los objetivos de cumplimiento de su empresa y la legislación, así como los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudarle en la conformidad:

- Guías de inicio rápido de seguridad y conformidad– estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA– este documento técnico describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- Recursos de conformidad de AWS – este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config – el servicio AWS Config evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS ofrece una vista integral de su estado de seguridad en AWS que le ayuda a comprobar la conformidad con las normas del sector de seguridad y las prácticas recomendadas.

Seguridad de la infraestructura en Amazon EC2 Container Registry

Al tratarse de un servicio administrado, Amazon EC2 Container Registry está protegido por los procedimientos de seguridad de red globales de AWS que se describen en el documento técnico Amazon Web Services: Información general sobre procesos de seguridad.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a Amazon ECR a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Le recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red, pero Amazon ECR admite políticas de acceso basadas en recursos, que pueden incluir restricciones en función de la dirección IP de origen. También puede utilizar las políticas de Amazon ECR para controlar el acceso desde puntos de enlace específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. Este proceso aísla con eficacia el acceso de red a un recurso de Amazon ECR determinado únicamente desde la VPC específica de la red de AWS. Para obtener más información, consulte Amazon ECR interfaces VPC de interfaz (AWS privatelink) (p. 95).

Amazon ECR interfaces VPC de interfaz (AWS privatelink)

Puede mejorar el estado de seguridad de su VPC configurando Amazon ECR para que utilice una interfaz de punto de enlace de la VPC. Los criterios de valoración VPC están impulsados por AWS privatelink, una tecnología que le permite acceder de forma privada Amazon ECR a través de direcciones IP privadas. AWS PrivateLink restringe todo el tráfico de red entre su VPC y Amazon ECR a la red de Amazon. No necesita una gateway de Internet, un dispositivo NAT ni una gateway privada virtual.

Para obtener más información sobre AWS puntos finales de privatelink y VPC, consulte Criterios de valoración VPC en el Guía del usuario de Amazon VPC.

Consideraciones para Amazon ECR Criterios de valoración VPC

Antes de configurar los puntos de enlace de la VPC para Amazon ECR, debe tener en cuenta las consideraciones siguientes.

- Para permitir Amazon ECS tareas que utilizan EC2 tipo de lanzamiento para extraer imágenes privadas de Amazon ECR, asegúrese de crear también los criterios de valoración VPC de interfaz para Amazon ECS. Para obtener más información, consulte Interfaces VPC de interfaz (AWS privatelink) en el Amazon Elastic Container Service Developer Guide.

  Important

  Amazon ECS tareas que utilizan Fargate tipo de lanzamiento no requiere el Amazon ECS interfaz de VPC de la interfaz.
- Amazon ECS tareas utilizando el Fargate el tipo de lanzamiento y la plataforma versión 1.3.0 o anterior solo requieren el com.amazonaws.***region***.ecr.dkr Amazon ECR el criterio de valoración VPC y el Amazon S3 terminal de enlace para aprovechar esta característica.
- Amazon ECS tareas utilizando el Fargate el tipo de lanzamiento y la plataforma versión 1.4.0 o posterior requieren tanto el com.amazonaws.***region***.ecr.dkr y com.amazonaws.***region***.ecr.api Amazon ECR Criterios de valoración VPC, así como el Amazon S3 terminal de enlace para aprovechar esta característica.
- Amazon ECS tareas utilizando el Fargate tipo de lanzamiento que extrae imágenes de contenedor de Amazon ECR puede restringir el acceso al VPC específico sus tareas utilizando y al terminal VPC el servicio se utiliza añadiendo claves de condición a la ejecución de la tarea IAM función para la tarea.

Para obtener más información, consulte Permisos IAM opcionales para tareas de Fargate que extraen imágenes ECR de Amazon sobre los criterios de valoración de interfaz en el Amazon Elastic Container Service Developer Guide.

- Amazon ECS tareas utilizando el Fargate tipo de lanzamiento que extrae imágenes de contenedor de Amazon ECR que también utilizan `awslogs` registrar controlador para enviar información de registro a CloudWatch Logs requiere el CloudWatch Logs Criterio de valoración VPC. Para obtener más información, consulte Crear el CloudWatch Logs criterio de valoración (p. 99).
- El grupo de seguridad asociado al punto de enlace de la VPC debe permitir las conexiones entrantes en el puerto 443 desde la subred privada de la VPC.
- Los puntos de enlace de la VPC no admiten las solicitudes entre regiones. Asegúrese de crear sus puntos de enlace de la VPC en la misma región en la que tiene previsto enviar llamadas a la API de Amazon ECR.
- Los puntos de enlace de la VPC solo admiten DNS proporcionadas por Amazon a través de Amazon Route 53. Si desea utilizar su propio DNS, puede utilizar el enrutamiento de DNS condicional. Para obtener más información, consulte Conjuntos de opciones DHCP en el Guía del usuario de Amazon VPC.
- Si sus contenedores tienen conexiones existentes con Amazon S3, sus conexiones pueden interrumpirse brevemente cuando se añade el Amazon S3 terminal de pasarela. Si desea evitar esta interrupción, cree un VPC nuevo que utilice el Amazon S3 terminal de enlace y luego migrar su Amazon ECS y sus contenedores en el nuevo VPC.

Consideraciones para las imágenes de Windows

Las imágenes basadas en el sistema operativo Windows incluyen artefactos restringidos por la licencia de distribuir. De forma predeterminada, al pulsar imágenes de Windows a un Amazon ECR repositorio, las capas que incluyen estos artefactos no se empujan a medida que se consideran capas extrañas. Cuando Microsoft proporciona los artefactos, las capas extrañas se recuperan de la infraestructura de Microsoft Azure. Por este motivo, para permitir que los contenedores puedan tirar de estas capas extrañas de Azure se necesitan pasos adicionales más allá de crear los terminales VPC.

Es posible anular este comportamiento al pulsar las imágenes de Windows para Amazon ECR utilizando el `--allow-nondistributable-artifacts` en el daemon de Docker. Cuando está activada, esta bandera se encargará de que las capas autorizadas se Amazon ECR que permite extraer estas imágenes de Amazon ECR a través del terminal VPC sin necesidad de acceso adicional a Azure.

> **Important**
>
> Uso de la `--allow-nondistributable-artifacts` La bandera no excluye su obligación de cumplir con los términos de la licencia de imagen base de contenedor de Windows; no puede publicar contenido de Windows para redistribución pública o de terceros. Se permite el uso dentro de su propio entorno.

Para habilitar el uso de esta marca para la instalación del acoplador, debe modificar el archivo de configuración del daemon de Docker, que, dependiendo de la instalación del acoplador, normalmente se puede configurar en el menú de configuración o preferencias debajo de la Motor de acoplador o editando la sección `C:\ProgramData\docker\config\daemon.json` archivo directamente.

A continuación se muestra un ejemplo de la configuración requerida. Sustituya el valor por el URI del repositorio que está llevando imágenes a.

```
{
    "allow-nondistributable-artifacts": [
        "111122223333.dkr.ecr.us-west-2.amazonaws.com"
    ]
}
```

Después de modificar el archivo de configuración del daemon de Docker, debe reiniciar el demonio de Docker antes de intentar pulsar la imagen. Confirme el impulso realizado verificando que la capa base se introdujo en el repositorio.

Note

Las capas base para las imágenes de Windows son grandes. El tamaño de la capa dará lugar a un mayor tiempo de empuje y de costes de almacenamiento adicionales en Amazon ECR para estas imágenes. Por estos motivos, recomendamos utilizar esta opción cuando sea estrictamente necesario reducir los tiempos de fabricación y los costes de almacenamiento actuales. Por ejemplo, el `mcr.microsoft.com/windows/servercore` la imagen tiene aproximadamente 1,7 gib de tamaño cuando se comprime en Amazon ECR.

Crear puntos de enlace de la VPC para Amazon ECR

Para crear los criterios de valoración VPC para el Amazon ECR servicio, utilice el Creación de un criterio de valoración de interfaz en el Guía del usuario de Amazon VPC.

Amazon ECS tareas utilizando el EC2 el tipo de lanzamiento requiere ambos Amazon ECR y el Amazon S3 terminal de pasarela.

Amazon ECS tareas utilizando el Fargate el tipo de lanzamiento y la plataforma versión 1.3.0 o anterior solo requieren el com.amazonaws.***region***.ecr.dkr Amazon ECR el criterio de valoración VPC y el Amazon S3 variables de la puerta de enlace.

Amazon ECS tareas utilizando el Fargate el tipo de lanzamiento y la plataforma versión 1.4.0 o posterior requieren tanto el com.amazonaws.***region***.ecr.dkr y com.amazonaws.***region***.ecr.api Amazon ECR Criterios de valoración VPC y el Amazon S3 variables de la puerta de enlace.

Note

El orden en el que se crean los puntos de enlace no importa.

com.amazonaws.***region***.ecr.dkr

Este punto de enlace se utiliza para las API de Docker Registry. Órdenes de cliente de Docker como `push` y `pull` utilice este criterio de valoración.

Cuando crea el com.amazonaws.***region***.ecr.dkr punto final, debe habilitar un nombre de host DNS privado. Para ello, asegúrese de que el Habilitar nombre DNS privado La opción está seleccionada en la consola VPC cuando crea el punto final VPC.

com.amazonaws.***region***.ecr.api

Note

El especificado *region* representa el identificador de región de un AWS Región admitida por Amazon ECR, como `us-east-2` para el Región EE.UU Este (Ohio).

Este criterio de valoración se utiliza para llamadas a la Amazon ECR API. Las acciones de la API, como DescribeImages y CreateRepositories, van a este punto de enlace.

Cuando el com.amazonaws.***region***.ecr.api se crea un criterio de valoración, tiene la opción de habilitar un nombre de host DNS privado. Active este ajuste seleccionando Habilitar nombre DNS privado en la consola VPC cuando cree el punto final VPC. Si habilita un nombre de host DNS privado para el terminal VPC, actualice su SDK o AWS CLI a la versión más reciente para especificar una URL de terminal al utilizar el SDK o AWS CLI no es necesario.

Si habilita un nombre de host DNS privado y está utilizando un SDK o AWS CLI versión publicada antes del 24 de enero de 2019, debe utilizar el `--endpoint-url` parámetro para especificar los

criterios de valoración de la interfaz. En el ejemplo siguiente se muestra el formato de la dirección URL del punto de enlace.

```
aws ecr create-repository --repository-name name --endpoint-url https://
api.ecr.region.amazonaws.com
```

Si no habilita un nombre de host de DNS privado para el punto de enlace de la VPC, debe utilizar el parámetro `--endpoint-url` que especifique el ID de punto de enlace de la VPC para el punto de enlace de interfaz. En el ejemplo siguiente se muestra el formato de la dirección URL del punto de enlace.

```
aws ecr create-repository --repository-name name --endpoint-url
 https://VPC_endpoint_ID.api.ecr.region.vpce.amazonaws.com
```

Crear el Amazon S3 terminal de pasarela

Para su Amazon ECS tareas para extraer imágenes privadas de Amazon ECR, debe crear un terminal de puerta de enlace para Amazon S3. El criterio de valoración de la puerta de enlace es obligatorio porque Amazon ECR usos Amazon S3 para almacenar las capas de imágenes. Cuando los contenedores descargan imágenes de Amazon ECR, deben acceder Amazon ECR para obtener el manifiesto de imagen y Amazon S3 para descargar las capas de imágenes reales. A continuación, se muestra el Nombre de recurso de Amazon (ARN) del bucket de Amazon S3 que contiene las capas para cada imagen de Docker:

```
arn:aws:s3:::prod-region-starport-layer-bucket/*
```

Utilice el Creación de un terminal de puerta de enlace en el Guía del usuario de Amazon VPC para crear lo siguiente Amazon S3 terminal de enlace para Amazon ECR. Cuando cree el punto de enlace, asegúrese de seleccionar las tablas de enrutamiento para su VPC.

com.amazonaws.*region*s3

El Amazon S3 endpoint usa un IAM documento de política para limitar el acceso al servicio. El Acceso completo se puede utilizar la política, ya que las restricciones que haya puesto en su tarea IAM funciones u otros IAM las políticas de usuario siguen siendo aplicables en la parte superior de esta política. Si desea limitar Amazon S3 acceso de cubo a los permisos mínimos requeridos para usar Amazon ECR, ver Permisos mínimos del bucket de Amazon S3 para Amazon ECR (p. 98).

Permisos mínimos del bucket de Amazon S3 para Amazon ECR

El Amazon S3 endpoint usa un IAM documento de política para limitar el acceso al servicio. Para permitir solo el mínimo Amazon S3 permisos de cubo para Amazon ECR, restringir el acceso a la Amazon S3 cubo que Amazon ECR utiliza cuando crea el IAM documento de política para el criterio de valoración.

En la siguiente tabla se describen los permisos de política de buckets de Amazon S3 necesarios para Amazon ECR.

Permiso	Descripción
`arn:aws:s3:::prod-region-starport-layer-bucket/*`	Proporciona acceso al bucket de Amazon S3 que contiene las capas para cada imagen de Docker. Representa el identificador de región de un AWS Región admitida por Amazon ECR, como `us-east-2` para el Región EE.UU Este (Ohio).

Example

El siguiente ejemplo ilustra cómo proporcionar acceso a la Amazon S3 cubos necesarios para Amazon ECR.

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::prod-region-starport-layer-bucket/*"]
    }
  ]
}
```

Crear el CloudWatch Logs criterio de valoración

Amazon ECS tareas utilizando el Fargate tipo de lanzamiento que utilice un VPC sin una puerta de enlace de Internet que también utilice el `awslogs` registrar controlador para enviar información de registro a CloudWatch Logs requiere que cree el com.amazonaws.*region*.registros interfaz VPC de interfaz para CloudWatch Logs. Para obtener más información, consulte Creación de un terminal de puerta de enlace en el Amazon CloudWatch Logs User Guide.

Cree una política de criterios de valoración para su Amazon ECR Criterios de valoración VPC

Una política de punto de enlace de la VPC es una política de recursos de IAM que se asocia a un punto de enlace al crearlo o modificarlo. Si no asocia una política al crear un punto de enlace, AWS asocia una política predeterminada que conceda acceso completo al servicio. Una política de punto de enlace no anula ni sustituye a las políticas de usuario de IAM ni las políticas específicas de los servicios. Se trata de una política independiente para controlar el acceso desde el punto de enlace al servicio especificado. Las políticas de punto de conexión deben escribirse en formato JSON. Para obtener más información, consulte Control del acceso a los servicios con los criterios de valoración VPC en el Guía del usuario de Amazon VPC.

Recomendamos crear una única IAM política de recursos y adjuntarla a ambos Amazon ECR Criterios de valoración de VPC.

A continuación, se muestra un ejemplo de una política de punto de enlace de Amazon ECR. Esta política permite a un rol específico de IAM extraer imágenes de Amazon ECR.

```
{
 "Statement": [{
  "Sid": "AllowPull",
  "Principal": {
   "AWS": "arn:aws:iam::1234567890:role/role_name"
  },
  "Action": [
   "ecr:BatchGetImage",
   "ecr:GetDownloadUrlForLayer"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

El siguiente ejemplo de política de punto de enlace impide que se elimine un repositorio especificado.

```
{
 "Statement": [{
   "Sid": "AllowAll",
   "Principal": "*",
   "Action": "*",
   "Effect": "Allow",
   "Resource": "*"
  },
  {
   "Sid": "PreventDelete",
   "Principal": "*",
   "Action": "ecr:DeleteRepository",
   "Effect": "Deny",
   "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
  }
 ]
}
```

El siguiente ejemplo de política de punto de enlace combina los dos ejemplos anteriores en una única política.

```
{
 "Statement": [{
   "Sid": "AllowAll",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "*",
   "Resource": "*"
  },
  {
   "Sid": "PreventDelete",
   "Effect": "Deny",
   "Principal": "*",
   "Action": "ecr:DeleteRepository",
   "Resource": "arn:aws:ecr:region:1234567890:repository/repository_name"
  },
  {
   "Sid": "AllowPull",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::1234567890:role/role_name"
   },
   "Action": [
    "ecr:BatchGetImage",
    "ecr:GetDownloadUrlForLayer"
   ],
   "Resource": "*"
  }
 ]
}
```

Para modificar la política de punto de enlace de la VPC para Amazon ECR

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Criterios de valoración.
3. Si aún no ha creado aún los puntos de enlace de la VPC para Amazon ECR, consulte Crear puntos de enlace de la VPC para Amazon ECR (p. 97).
4. Seleccione el Amazon ECR VPC endpoint to add a policy to, and choose the Política en la mitad inferior de la pantalla.

5. Elegir Editar política y realizar los cambios en la política.
6. Elegir Guardar para guardar la política.

Monitorización de Amazon ECR

Puede monitorear las instancias de uso de las API de Amazon ECR con Amazon CloudWatch, que recopila y procesa los datos sin formato de Amazon ECR y los convierte en métricas legibles prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de dos semanas para que pueda obtener acceso a información histórica y obtener una mejor perspectiva del uso de las API. Los datos de las métricas de Amazon ECR se envían automáticamente a CloudWatch en periodos de un minuto. Para obtener más información sobre CloudWatch, consulte la Guía del usuario de Amazon CloudWatch.

Amazon ECR dispone de métricas sobre el uso de las API en acciones de autorización, inserción de imágenes y extracción de imágenes.

El monitoreo es una parte importante para mantener la fiabilidad, la disponibilidad y el rendimiento de Amazon ECR y las soluciones de AWS. Le recomendamos que recopile datos de monitoreo de los recursos que conforman la solución de AWS para que pueda depurar con mayor facilidad un error de varios puntos, en caso de que se produzca alguno. No obstante, antes de comenzar a monitorear Amazon ECR, debe crear un plan que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de monitorización va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitorización?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del rendimiento normal de Amazon ECR en su entorno. Para ello, debe medirse el rendimiento en distintos momentos y bajo distintas condiciones de carga. A medida que monitoree Amazon ECR, guarde los datos de monitorización históricos para que pueda compararlos con los datos de rendimiento actual, identificar los patrones de rendimiento normal y las anomalías en el rendimiento, así como desarrollar métodos para la resolución de problemas.

Temas

Visualización de las cuotas de servicio y configuración de alarmas

Puede utilizar la consola de CloudWatch para visualizar las cuotas de servicio y compararlas con el uso actual. También puede configurar alarmas para recibir notificaciones cuando se acerque a una cuota.

Para visualizar una cuota de servicio y, opcionalmente, configurar una alarma

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics.
3. En la pestaña All metrics (Todas las métricas), elija Usage (Uso) y, a continuación, By AWS Resource (Por recurso de AWS).

   Aparecerá la lista de métricas de uso de cuotas de servicio.
4. Active la casilla situada junto a una de las métricas.

   En el gráfico se muestra su uso actual de ese recurso de AWS.
5. Para añadir su cuota de servicio al gráfico, haga lo siguiente:

   a. Elija la pestaña Graphed metrics.
   b. Elija Math expression (Expresión matemática) y Start with an empty expression (Comenzar con una expresión vacía). A continuación, en la nueva fila, en Details (Detalles), escriba **`SERVICE_QUOTA(m1)`**.

      Se añade una nueva línea al gráfico, mostrando la cuota de servicio del recurso representado en la métrica.
6. Para ver su uso actual como porcentaje de la cuota, añada una nueva expresión o cambie la expresión SERVICE_QUOTA actual. En el caso de la nueva expresión, use **`m1/60/SERVICE_QUOTA(m1)*100`**
7. (Opcional) Para configurar una alarma que le notifique si se acerca a la cuota de servicio, haga lo siguiente:

   a. En la fila **`m1/60/SERVICE_QUOTA(m1)*100`**, en Actions (Acciones), elija el icono de alarma. Se parece a una campana.

      Aparecerá la página de creación de alarmas.
   b. En Conditions (Condiciones), asegúrese de que Threshold type (Tipo de umbral) es Static (Estático) y Whenever Expression1 is (Siempre que Expression1 sea) se establece en Greater (Mayor). Por debajo de de, introduzca **`80`**. Esto crea una alarma que pasa al estado ALARM cuando el uso supera el 80 por ciento de la cuota.
   c. Seleccione Next (Siguiente).
   d. En la página siguiente, seleccione un tema de Amazon SNS o cree uno nuevo. Este tema se notifica cuando la alarma pasa al estado ALARM. A continuación, elija Next (Siguiente).
   e. En la página siguiente, escriba un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
   f. Elija Create alarm (Crear alarma).

Métricas de uso de Amazon ECR

Puede utilizar las métricas de uso de CloudWatch para proporcionar visibilidad sobre el uso de los recursos de su cuenta. Utilice estas métricas para visualizar el uso actual del servicio en paneles y gráficos de CloudWatch.

Las métricas de uso de Amazon ECR se corresponden con las cuotas de servicio de AWS. Puede configurar alarmas que le avisen cuando su uso se acerque a una cuota de servicio. Para obtener más información acerca de las cuotas de servicio de Amazon ECR, consulteAmazon ECRCuotas de servicio de (p. 115).

Amazon ECR publica las siguientes métricas en el espacio de nombres `AWS/Usage`.

Métrica	Descripción
`CallCount`	Número de llamadas de acciones de la API realizadas desde la cuenta. Los recursos se definen por las dimensiones asociadas a la métrica. La estadística más útil de esta métrica es `SUM`, que representa la suma de los valores de todas las contribuciones durante el período definido.

Las siguientes dimensiones se utilizan para ajustar las métricas de uso publicadas por Amazon ECR.

Dimensión	Descripción
`Service`	El nombre del servicio de AWS que contiene el recurso. Para las métricas de uso de Amazon ECR, el valor de esta dimensión es `ECR`.
`Type`	El tipo de entidad que se registra. Actualmente, el único valor válido para las métricas de uso de Amazon ECR es `API`.
`Resource`	El tipo de recurso que se está ejecutando. Actualmente, Amazon ECR devuelve información sobre el uso de la API en relación con las siguientes acciones. • GetAuthorizationToken • BatchCheckLayerAvailability • InitiateLayerUpload • UploadLayerPart • CompleteLayerUpload • PutImage • BatchGetImage • GetDownloadUrlForLayer
`Class`	La clase de recurso del que se realiza el seguimiento. En la actualidad, Amazon ECR no utiliza la dimensión de clase.

Informes de uso de Amazon ECR

AWS proporciona una herramienta de elaboración de informes gratuita denominada Cost Explorer que le permite analizar el costo y el uso de los recursos de Amazon ECR.

Utilice Cost Explorer para ver gráficos sobre el uso y los costos. Puede ver los datos de los 13 meses anteriores y predecir la cantidad que probablemente va a gastar durante los tres meses siguientes. Puede utilizar el Cost Explorer para ver sus patrones de gasto en recursos de AWS a lo largo del tiempo, identificar aspectos que deben estudiarse más a fondo y consultar tendencias que le pueden ayudar a comprender los costos. También puede especificar intervalos de tiempo en los datos y ver los datos temporales por día o por mes.

Los datos de medición de los informes de uso y costos muestran el uso en todos los repositorios de Amazon ECR. Para obtener más información, consulte Etiquetado de los recursos para facturación (p. 36).

Para obtener más información sobre cómo crear un Informe de uso y costos de AWS, consulte Informes de uso y costo de AWS en la Guía del usuario de AWS Billing and Cost Management.

Amazon ECR y EventBridge

Amazon EventBridge le permite automatizar los servicios de AWS y responder automáticamente a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios de recursos. Los eventos de los servicios de AWS se envían a EventBridge casi en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés e incluir las acciones automatizadas que deben realizarse cuando un evento cumpla una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Agregar eventos a grupos de registros en CloudWatch Logs
- Invocar una función de AWS Lambda
- Invocar Ejecutar comando de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activar una máquina de estado de AWS Step Functions
- Notificar un tema de Amazon SNS o una cola de AWS SMS

Para obtener más información, consulte Introducción a Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Eventos de ejemplo de Amazon ECR

Los siguientes son los eventos de ejemplo de Amazon ECR.

Evento para una inserción de imagen completada

El siguiente evento se envía cuando se completa cada inserción de imagen. Para obtener más información, consulte Inserción de una imagen de Docker (p. 39).

```
{
    "version": "0",
    "id": "13cde686-328b-6117-af20-0e5566167482",
    "detail-type": "ECR Image Action",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-11-16T01:54:34Z",
    "region": "us-west-2",
    "resources": [],
    "detail": {
        "result": "SUCCESS",
        "repository-name": "my-repo",
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "action-type": "PUSH",
        "image-tag": "latest"
    }
}
```

Evento para una exploración de imagen completada

El siguiente evento se envía cuando se completa cada escaneo de imagen. El parámetro `finding-severity-counts` solo devolverá un valor para un nivel de gravedad, si existe. Por ejemplo, si la imagen no contiene resultados de nivel `CRITICAL`, no se devolverá ningún recuento crítico. Para obtener más información, consulte Escaneo de imágenes (p. 59).

```
{
```

```
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "ECR Image Scan",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-10-29T02:36:48Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:123456789012:repository/my-repo"
    ],
    "detail": {
        "scan-status": "COMPLETE",
        "repository-name": "my-repo",
        "finding-severity-counts": {
        "CRITICAL": 10,
        "MEDIUM": 9
      },
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "image-tags": []
    }
}
```

Evento para una eliminación de imagen

El siguiente evento se envía cuando se elimina una imagen. Para obtener más información, consulte Eliminar una imagen (p. 44).

```
{
    "version": "0",
    "id": "dd3b46cb-2c74-f49e-393b-28286b67279d",
    "detail-type": "ECR Image Action",
    "source": "aws.ecr",
    "account": "123456789012",
    "time": "2019-11-16T02:01:05Z",
    "region": "us-west-2",
    "resources": [],
    "detail": {
        "result": "SUCCESS",
        "repository-name": "my-repo",
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "action-type": "DELETE",
        "image-tag": "latest"
    }
}
```

Registro Amazon ECR acciones con AWS CloudTrail

Amazon ECR está integrado en AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon ECR. CloudTrail captura las acciones de Amazon ECR como eventos.

- Todas las llamadas a la API, incluidas las llamadas desde la consola de Amazon ECR
- Todas las acciones realizadas debido a la configuración de cifrado en sus repositorios de
- Todas las acciones realizadas debido a las reglas de la directiva del ciclo de vida, incluidas las acciones correctas y las que no tienen éxito

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon ECR. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante esta información, puede determinar la solicitud que se envió a Amazon ECR, la dirección IP de origen, quién realizó la solicitud, cuándo y detalles adicionales.

Para obtener más información, consulte AWS CloudTrail User Guide.

Información de Amazon ECR en CloudTrail

CloudTrail se habilita en su cuenta de AWS al crearla. Cuando se produce una actividad en Amazon ECR, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en el Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Amazon ECR, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. Al crear un registro de seguimiento en la consola, puede aplicarlo a una sola región o a todas las regiones. El registro de seguimiento registra los eventos de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También puede configurar otros servicios de AWS para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- Creación de un registro de seguimiento de su cuenta de AWS
- Integración de servicios de AWS con registros de CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de la API de Amazon ECR, que se documentan en la Amazon EC2 Container Registry API Reference. Cuando realiza tareas comunes, en los archivos de registro de CloudTrail se generan secciones sobre cada una de las acciones de API que participan en esa tarea. Por ejemplo, cuando crea un repositorio, se generan las secciones `GetAuthorizationToken`, `CreateRepository` y `SetRepositoryPolicy` en los archivos de registro de CloudTrail. Cuando inserta una imagen en un repositorio, se generan las secciones `InitiateLayerUpload`, `UploadLayerPart`, `CompleteLayerUpload` y `PutImage`. Cuando extrae una imagen, se generan las secciones `GetDownloadUrlForLayer` y `BatchGetImage`. Si desea ver ejemplos de estas tareas comunes, consulte CloudTrail ejemplos de entradas de registro (p. 108).

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del nodo raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento `userIdentity` de CloudTrail.

Descripción de las entradas de los archivos de registro de Amazon ECR

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro al bucket de Amazon S3 que se especifique. Los archivos de registro de CloudTrail contienen

una o varias entradas de registro. Un evento representa una solicitud específica de un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no conforman un seguimiento ordenado de la pila de las llamadas a la API públicas, por lo que no aparecen en ningún orden específico.

CloudTrail ejemplos de entradas de registro

Estos son ejemplos de entradas de registro de CloudTrail correspondientes a algunas tareas comunes de Amazon ECR.

> **Note**
>
> Estos ejemplos se han manipulado para mejorar la legibilidad. En un archivo de registro de CloudTrail, todas las entradas y eventos aparecen en la misma línea. Además, este ejemplo se ha limitado a una única entrada de Amazon ECR. En un archivo de registro de CloudTrail real, ve las entradas y los eventos de varios servicios de AWS.

Temas

Ejemplo: Crear acción de repositorio

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail donde se muestra la acción `CreateRepository`.


```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
        "arn": "arn:aws:sts::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-07-11T21:54:07Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            }
        }
    },
    "eventTime": "2018-07-11T22:17:43Z",
    "eventSource": "ecr.amazonaws.com",
    "eventName": "CreateRepository",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "repositoryName": "testrepo"
```

```
    },
    "responseElements": {
        "repository": {
            "repositoryArn": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
            "repositoryName": "testrepo",
            "repositoryUri": "123456789012.dkr.ecr.us-east-2.amazonaws.com/testrepo",
            "createdAt": "Jul 11, 2018 10:17:44 PM",
            "registryId": "123456789012"
        }
    },
    "requestID": "cb8c167e-EXAMPLE",
    "eventID": "e3c6f4ce-EXAMPLE",
    "resources": [
        {
            "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
            "accountId": "123456789012"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


Ejemplo: AWS KMS Acción de API CreateGrant al crear un Amazon ECR repositorio

El siguiente ejemplo muestra una CloudTrail que muestra la entrada de registro de AWS KMS Acción CreateGrant al crear un Amazon ECR El repositorio de con el cifrado de KMS habilitado. Para cada repositorio que se crea con el cifrado de KMS habilitado, debería ver dos entradas de registro de CreateGrant en CloudTrail.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP6W46J43IG7LXAQ",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "sessionIssuer": {

            },
            "webIdFederationData": {

            },
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-06-10T19:22:10Z"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-06-10T19:22:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "keyId": "4b55e5bf-39c8-41ad-b589-18464af7758a",
        "granteePrincipal": "ecr.us-west-2.amazonaws.com",
        "operations": [
```

```
            "GenerateDataKey",
            "Decrypt"
        ],
        "retiringPrincipal": "ecr.us-west-2.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {
                "aws:ecr:arn": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo"
            }
        }
    },
    "responseElements": {
        "grantId": "3636af9adfee1accb67b83941087dcd45e7fadc4e74ff0103bb338422b5055f3"
    },
    "requestID": "047b7dea-b56b-4013-87e9-a089f0f6602b",
    "eventID": "af4c9573-c56a-4886-baca-a77526544469",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:123456789012:key/4b55e5bf-39c8-41ad-
b589-18464af7758a"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Ejemplo: Acción de inserción de imagen

El ejemplo siguiente muestra una entrada de registro de CloudTrail en la que se puede ver el envío de una imagen con la acción `PutImage`.

> **Note**
>
> Cuando envíe una imagen, verá también las referencias `InitiateLayerUpload`, `UploadLayerPart` y `CompleteLayerUpload` en los registros de CloudTrail.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Mary_Major",
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2019-04-15T16:42:14Z"
   }
  }
 },
 "eventTime": "2019-04-15T16:45:00Z",
 "eventSource": "ecr.amazonaws.com",
 "eventName": "PutImage",
 "awsRegion": "us-east-2",
 "sourceIPAddress": "203.0.113.12",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "repositoryName": "testrepo",
  "imageTag": "latest",
  "registryId": "123456789012",
```

```
  "imageManifest": "{\n   \"schemaVersion\": 2,\n   \"mediaType\": \"application/
vnd.docker.distribution.manifest.v2+json\",\n   \"config\": {\n      \"mediaType\":
 \"application/vnd.docker.container.image.v1+json\",\n      \"size\": 5543,\n
 \"digest\": \"sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
\"\n   },\n   \"layers\": [\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 43252507,\n
 \"digest\": \"sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 846,\n         \"digest
\": \"sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 615,\n         \"digest
\": \"sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 850,\n         \"digest
\": \"sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 168,\n         \"digest
\": \"sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 37720774,\n         \"digest
\": \"sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 30432107,\n
 \"digest\": \"sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 197,\n         \"digest
\": \"sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecfe7d
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 154,\n         \"digest
\": \"sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 176,\n         \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 183,\n         \"digest
\": \"sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest
\": \"sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 212,\n         \"digest\":
 \"sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629\"\n      }\n
  ]\n}"
 },
 "responseElements": {
  "image": {
   "repositoryName": "testrepo",
   "imageManifest": "{\n   \"schemaVersion\": 2,\n   \"mediaType\": \"application/
vnd.docker.distribution.manifest.v2+json\",\n   \"config\": {\n      \"mediaType\":
 \"application/vnd.docker.container.image.v1+json\",\n      \"size\": 5543,\n
 \"digest\": \"sha256:000b9b805af1cdb60628898c9f411996301a1c13afd3dbef1d8a16ac6dbf503a
\"\n   },\n   \"layers\": [\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 43252507,\n
 \"digest\": \"sha256:3b37166ec61459e76e33282dda08f2a9cd698ca7e3d6bc44e6a6e7580cdeff8e
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 846,\n         \"digest
\": \"sha256:504facff238fde83f1ca8f9f54520b4219c5b8f80be9616ddc52d31448a044bd
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 615,\n         \"digest
\": \"sha256:ebbcacd28e101968415b0c812b2d2dc60f969e36b0b08c073bf796e12b1bb449\"\n
      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 850,\n         \"digest
\": \"sha256:c7fb3351ecad291a88b92b600037e2435c84a347683d540042086fe72c902b8a
\"\n      },\n      {\n         \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n         \"size\": 168,\n         \"digest
```

\": \"sha256:2e3debadcbf7e542e2aefbce1b64a358b1931fb403b3e4aeca27cb4d809d56c2\"\n
      },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 37720774,\n   \"digest
\": \"sha256:f8c9f51ad524d8ae9bf4db69cd3e720ba92373ec265f5c390ffb21bb0c277941\"\n
      },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 30432107,\n
 \"digest\": \"sha256:813a50b13f61cf1f8d25f19fa96ad3aa5b552896c83e86ce413b48b091d7f01b
\"\n   },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 197,\n   \"digest
\": \"sha256:7ab043301a6187ea3293d80b30ba06c7bf1a0c3cd4c43d10353b31bc0cecfe7d
\"\n   },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 154,\n   \"digest
\": \"sha256:67012cca8f31dc3b8ee2305e7762fee20c250513effdedb38a1c37784a5a2e71\"\n
      },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 176,\n   \"digest
\": \"sha256:3bc892145603fffc9b1c97c94e2985b4cb19ca508750b15845a5d97becbd1a0e
\"\n   },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 183,\n   \"digest
\": \"sha256:6f1c79518f18251d35977e7e46bfa6c6b9cf50df2a79d4194941d95c54258d18\"\n
      },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 212,\n   \"digest
\": \"sha256:b7bcfbc2e2888afebede4dd1cd5eebf029bb6315feeaf0b56e425e11a50afe42\"\n
      },\n   {\n   \"mediaType\": \"application/
vnd.docker.image.rootfs.diff.tar.gzip\",\n   \"size\": 212,\n   \"digest\":
 \"sha256:2b220f8b0f32b7c2ed8eaafe1c802633bbd94849b9ab73926f0ba46cdae91629\"\n   }\n
  ]\n}",
   "registryId": "123456789012",
   "imageId": {
    "imageDigest":
 "sha256:98c8b060c21d9adbb6b8c41b916e95e6307102786973ab93a41e8b86d1fc6d3e",
    "imageTag": "latest"
   }
  }
 },
 "requestID": "cf044b7d-5f9d-11e9-9b2a-95983139cc57",
 "eventID": "2bfd4ee2-2178-4a82-a27d-b12939923f0f",
 "resources": [{
  "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
  "accountId": "123456789012"
 }],
 "eventType": "AwsApiCall",
 "recipientAccountId": "123456789012"
}

Ejemplo: Acción de extracción de imagen

El ejemplo siguiente muestra una entrada de registro de CloudTrail en la que se puede ver que se ha extraído una imagen con la acción `BatchGetImage`.

> **Note**
>
> Cuando extraiga una imagen, si aún no la tiene localmente, verá también referencias `GetDownloadUrlForLayer` en los registros de CloudTrail.

{
    "eventVersion": "1.04",
    "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
    "arn": "arn:aws:sts::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Mary_Major",
  "sessionContext": {

```
   "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2019-04-15T16:42:14Z"
   }
  }
 },
 "eventTime": "2019-04-15T17:23:20Z",
 "eventSource": "ecr.amazonaws.com",
 "eventName": "BatchGetImage",
 "awsRegion": "us-east-2",
 "sourceIPAddress": "203.0.113.12",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
  "imageIds": [{
   "imageTag": "latest"
  }],
  "acceptedMediaTypes": [
   "application/json",
   "application/vnd.oci.image.manifest.v1+json",
   "application/vnd.oci.image.index.v1+json",
   "application/vnd.docker.distribution.manifest.v2+json",
   "application/vnd.docker.distribution.manifest.list.v2+json",
   "application/vnd.docker.distribution.manifest.v1+prettyjws"
  ],
  "repositoryName": "testrepo",
  "registryId": "123456789012"
 },
 "responseElements": null,
 "requestID": "2a1b97ee-5fa3-11e9-a8cd-cd2391aeda93",
 "eventID": "c84f5880-c2f9-4585-9757-28fa5c1065df",
 "resources": [{
  "ARN": "arn:aws:ecr:us-east-2:123456789012:repository/testrepo",
  "accountId": "123456789012"
 }],
 "eventType": "AwsApiCall",
 "recipientAccountId": "123456789012"
}
```


Ejemplo: Acción de política de ciclo de vida de imagen

En el siguiente ejemplo se muestra una entrada de registro de CloudTrail que muestra cuándo caduca una imagen debido a una regla de directiva de ciclo de vida. Este tipo de evento se puede encontrar filtrando por `PolicyExecutionEvent` en el campo de nombre del evento.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-03-12T20:22:12Z",
    "eventSource": "ecr.amazonaws.com",
    "eventName": "PolicyExecutionEvent",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "9354dd7f-9aac-4e9d-956d-12561a4923aa",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:ecr:us-west-2:123456789012:repository/testrepo",
            "accountId": "123456789012",
```

```
            "type": "AWS::ECR::Repository"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "repositoryName": "testrepo",
        "lifecycleEventPolicy": {
            "lifecycleEventRules": [
                {
                    "rulePriority": 1,
                    "description": "remove all images > 2",
                    "lifecycleEventSelection": {
                        "tagStatus": "Any",
                        "tagPrefixList": [],
                        "countType": "Image count more than",
                        "countNumber": 2
                    },
                    "action": "expire"
                }
            ],
            "lastEvaluatedAt": 0,
            "policyVersion": 1,
            "policyId": "ceb86829-58e7-9498-920c-aa042e33037b"
        },
        "lifecycleEventImageActions": [
            {
                "lifecycleEventImage": {
                    "digest":
 "sha256:ddba4d27a7ffc3f86dd6c2f92041af252a1f23a8e742c90e6e1297bfa1bc0c45",
                    "tagStatus": "Tagged",
                    "tagList": [
                        "alpine"
                    ],
                    "pushedAt": 1584042813000
                },
                "rulePriority": 1
            },
            {
                "lifecycleEventImage": {
                    "digest":
 "sha256:6ab380c5a5acf71c1b6660d645d2cd79cc8ce91b38e0352cbf9561e050427baf",
                    "tagStatus": "Tagged",
                    "tagList": [
                        "centos"
                    ],
                    "pushedAt": 1584042842000
                },
                "rulePriority": 1
            }
        ]
    }
}
```

Amazon ECRCuotas de servicio de

En la tabla siguiente , se muestran las cuotas de servicio predeterminadas de Amazon EC2 Container Registry (Amazon ECR).

Cuota de servicio	Descripción	Valor de cuota predeterminado
Repositorios registrados	El número máximo de repositorios que puede crear por región.	10 000
Imagen por repositorio	El número máximo de imágenes por repositorio.	10 000

En la tabla siguiente, se muestran las cuotas de velocidad predeterminadas de cada una de las acciones de API de Amazon ECR implicadas en la inserción y extracción de imágenes.

Amazon ECRAcción de	Operación de la API	Descripción	Valor de cuota predeterminado
Autenticación	Tasa de solicitudes GetAuthorizationToken	La tasa de solicitudes de la API GetAuthorizationToken que se pueden realizar por segundo y por región.	$200
Inserción de imágenes	Tasa de solicitudes de BatchCheckLayerAvailability	La tasa de solicitudes de la API BatchCheckLayerAvailability que se pueden realizar por segundo y por región. Cuando se inserta una imagen en un repositorio, se comprueba cada capa de la imagen para verificar si se ha cargado antes. Si ya se ha cargado, se omite.	$200
	Tasa de solicitudes de InitiateLayerUpload	La tasa de solicitudes de la API InitiateLayerUpload que se pueden realizar por segundo y por región. Cuando se inserta una imagen, se llama una vez a la API InitiateLayerUpload por	-10

Amazon ECRAcción de	Operación de la API	Descripción	Valor de cuota predeterminado
		capa de la imagen que aún no se ha cargado. La acción de la API BatchCheckLayerAvailability determina si la capa de la imagen se ha cargado o no.	
	Tasa de solicitudes de CompleteLayerUpload	La tasa de solicitudes de la API CompleteLayerUpload que se pueden realizar por segundo y por región. Cuando se inserta una imagen, se llama una vez a la API CompleteLayerUpload por cada capa nueva de la imagen para comprobar si la carga se ha completado.	-10
	Tasa de solicitudes de UploadLayerPart	La tasa de solicitudes de la API UploadLayerPart que se pueden realizar por segundo y por región. Cuando se inserta una imagen, cada capa nueva de la imagen se carga en partes. El tamaño máximo de cada parte de la capa de imagen puede ser de 20 971 520 bytes (o de unos 20 MB). La API UploadLayerPart se invoca una vez por cada nueva parte de la capa de imagen.	260

Amazon ECRAcción de	Operación de la API	Descripción	Valor de cuota predeterminado
	Tasa de solicitudes de PutImage	La tasa de solicitudes de la API PutImage que se pueden realizar por segundo y por región. Cuando se inserta una imagen y se han cargado todas las capas nuevas de la imagen, se llama una vez a la API PutImage para crear o actualizar el manifiesto de la imagen y las etiquetas asociadas a la imagen.	-10
Extracción de imágenes	Tasa de solicitudes de BatchGetImage	La tasa de solicitudes de la API BatchGetImage que se pueden realizar por segundo y por región. Cuando se extrae una imagen, se llama una vez a la API BatchGetImage para recuperar el manifiesto de la imagen.	1 000
	Tasa de solicitudes de GetDownloadUrlForLayer	La tasa de solicitudes de la API GetDownloadUrlForLayer que se pueden realizar por segundo y por región. Cuando se extrae una imagen, se llama una vez a la API GetDownloadUrlForLayer por capa de la imagen que aún no está almacenada en caché.	1500

En la tabla siguiente, se muestran otras cuotas de las imágenes de Amazon ECR y Docker que no se pueden modificar.

> **Note**
>
> La información de la parte de la capa mencionada en la tabla siguiente solo se aplica a los clientes que llaman directamente a las acciones de las API de Amazon ECR para comenzar cargas multiparte en operaciones de inserción de imágenes. Esta acción es poco habitual. Es recomendable que utilice la CLI de Docker para extraer, etiquetar e insertar imágenes.

Cuota de servicio	Descripción	Valor de la cuota
Partes de capa	El número máximo de partes de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon Amazon ECR directamente para comenzar cargas multiparte para operaciones de inserción de imágenes.	1 000
Tamaño máximo de capa	Tamaño máximo (MiB) de una capa. **	10 000
Tamaño mínimo de parte de la capa	Tamaño mínimo (MiB) de una parte de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon Amazon ECR directamente para comenzar cargas multiparte para operaciones de inserción de imágenes.	5
Tamaño máximo de parte de la capa	Tamaño máximo (MiB) de una parte de capa. Esto solo es aplicable si utiliza las acciones de la API de Amazon Amazon ECR directamente para comenzar cargas multiparte para operaciones de inserción de imágenes.	-10
Etiquetas por imagen	El número máximo de etiquetas por imagen.	1000*
Duración de la política del ciclo de vida	Número máximo de caracteres en una política de ciclo de vida.	30 720
Reglas por política de ciclo de vida	El número máximo de reglas en una política de ciclo de vida.	50.
Tasa de escaneos de imágenes	El número máximo de escaneos de imágenes por imagen y día.	-1

** El tamaño máximo de capa indicado aquí se calcula multiplicando el tamaño máximo de la parte de capa (10 MiB) por el número máximo de partes de capa (1 000).

Gestionar su Amazon ECR cuotas de servicio en el Consola de administración de AWS

Amazon ECR se ha integrado con Cuotas de servicio, un AWS servicio que le permite ver y gestionar sus cuotas desde una ubicación central. Para obtener más información, consulte ¿Qué son las cuotas de servicio? en el Guía del usuario de Cuotas de servicio.

Cuotas de servicioCon Amazon ECR, resulta más fácil buscar el valor de todas las cuotas de servicio de .

Para ver Amazon ECR cuotas de servicio (Consola de administración de AWS)

1. Abra la consola de Cuotas de servicio en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, seleccione Servicios AWS.
3. Desde el AWS servicios lista, buscar y seleccionar Amazon EC2 Container Registry (Amazon ECR).

   En el Cuotas de servicio puede ver el nombre de cuota de servicio, el valor aplicado (si está disponible), AWS cuota predeterminada y si el valor de cuota es ajustable.
4. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en el Guía del usuario de Cuotas de servicio.

Creación de una alarma de CloudWatch para monitorear las métricas de uso de las API

Amazon ECR proporciona CloudWatch indicadores de uso que corresponden al AWS cuotas de servicio para cada una de las apis implicadas en la autenticación del registro, la inserción de imágenes y las acciones de extracción de imágenes. En la consola de Cuotas de servicio, puede ver el uso en gráficos y configurar alarmas que le avisen cuando este se aproxime a una cuota de servicio. Para obtener más información, consulte Métricas de uso de Amazon ECR (p. 103).

Siga los pasos siguientes para crear un CloudWatch basada en una de las Amazon ECR Métricas de uso de API.

Para crear una alarma basada en su Amazon ECR cuotas de uso (Consola de administración de AWS)

1. Abra la consola de Cuotas de servicio en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, seleccione Servicios AWS.
3. Desde el AWS servicios lista, buscar y seleccionar Amazon EC2 Container Registry (Amazon ECR).
4. En el Cuotas de servicio seleccione la lista Amazon ECR cuota de uso que desea crear una alarma para.
5. En el Amazon CloudWatch Events sección de alarmas, elegir Crear.
6. Para Umbral de alarma, seleccione el porcentaje del valor de cuota aplicado que desea establecer como valor de alarma.
7. Para Nombre de alarma, introduzca un nombre para la alarma y, a continuación, elija Crear.

Amazon ECRSolución de problemas de

En este capítulo se proporciona ayuda para encontrar información de diagnóstico de Amazon EC2 Container Registry (Amazon ECR) y pasos para resolver problemas y saber cómo actuar con mensajes de error comunes.

Temas

Habilitar el resultado de depuración en Docker

Para comenzar a solucionar cualquier problema relacionado con Docker, habilite primero el resultado de depuración del demonio de Docker en las instancias de host. Para obtener más información sobre la activación de la depuración del acoplador si está utilizando imágenes de Amazon ECR sobre el Amazon ECS instancias de contenedor, ver Activación de la salida de depuración del acoplador en el Amazon Elastic Container Service Developer Guide.

Habilitar AWS CloudTrail

Información adicional sobre los errores devueltos por Amazon ECR se puede detectar mediante la habilitación AWS CloudTrail, que es un servicio que registra AWS llamadas para su cuenta de AWS. CloudTrail envía archivos de registro a un Amazon S3 cubo. Utilice la información recopilada por CloudTrail para ver las solicitudes que se han realizado correctamente a los servicios de AWS, quiénes las han hecho, cuándo, etc. Para obtener más información sobre CloudTrail, entre ella cómo activarlo y encontrar los archivos de registro, consulte la AWS CloudTrail User Guide. Para obtener más información sobre el uso de CloudTrail con Amazon ECR, ver Registro Amazon ECR acciones con AWS CloudTrail (p. 106).

Optimizar el desempeño en Amazon ECR

En la siguiente sección se facilita información sobre las configuraciones y estrategias que se pueden aplicar para optimizar el desempeño al utilizar Amazon ECR.

Usar Docker 1.10 o versiones posteriores para poder realizar cargas en capas simultáneas

Las imágenes de Docker se componen de capas, que son etapas intermedias de compilación de la imagen. Cada línea de un archivo Dockerfile genera una nueva capa. Al utilizar Docker 1.10 o versiones posteriores, Docker envía de forma predeterminada tantas capas como cargas simultáneas sea posible enviar a Amazon ECR, lo que reduce el tiempo de carga.

Usar una imagen base más pequeña

Las imágenes predeterminadas disponibles en Docker Hub pueden contener varias dependencias que no son necesarias para la aplicación. Plantéese utilizar una imagen más pequeña creada y mantenida

por otros miembros de la comunidad Docker o cree su propia imagen base a partir de la imagen de prueba mínima de Docker. Para obtener más información, consulte Crear una imagen base en la documentación de Docker.

Sitúe las dependencias que menos cambian en la primera parte del archivo Dockerfile

Docker almacena capas en caché, lo que incrementa la velocidad de compilación. Si una capa no ha cambiado desde la última compilación, Docker recurre a la versión en caché en lugar de compilarla de nuevo. Sin embargo, cada capa depende de las que le anteceden. Si una capa cambia, Docker compila de nuevo no solo esa capa, sino también las que le siguen.

Para reducir al mínimo el tiempo necesario para compilar de nuevo un archivo Docker y volver a cargar las capas, plantéese situar las dependencias que cambian con menos frecuencia en el archivo Docker. Sitúe las dependencias que cambian rápidamente (como, por ejemplo, el código fuente de la aplicación) más adelante en la pila.

Encadene los comandos para evitar almacenar archivos innecesarios.

Los archivos intermedios que se crean en una capa siguen formando parte de ella aunque se eliminen en una capa posterior. Considere el siguiente ejemplo:

```
WORKDIR /tmp
RUN wget http://example.com/software.tar.gz
RUN wget tar -xvf software.tar.gz
RUN mv software/binary /opt/bin/myapp
RUN rm software.tar.gz
```

En este ejemplo, las capas creadas por el primer y el segundo comando RUN contienen el archivo original .tar.gz y su contenido descomprimido. Esto ocurre a pesar de que el cuarto comando RUN elimina el archivo .tar.gz. Estos comandos se pueden encadenar en una única instrucción RUN para asegurarse de que los archivos innecesarios no formen parte de la imagen final de Docker:

```
WORKDIR /tmp
RUN wget http://example.com/software.tar.gz &&\
    wget tar -xvf software.tar.gz &&\
    mv software/binary /opt/bin/myapp &&\
    rm software.tar.gz
```

Usar el punto de enlace regional más cercano

Para reducir la latencia al extraer imágenes de Amazon ECR, utilice el punto de enlace regional más cercano a la zona de ejecución de la aplicación. Si la aplicación se ejecuta en una instancia Amazon EC2, use el código shell a continuación para obtener la región de la zona de disponibilidad de la instancia:

```
REGION=$(curl -s http://169.254.169.254/latest/meta-data/placement/availability-zone |\
     sed -n 's/\(\d*\)[a-zA-Z]*$/\1/p')
```

La región puede pasarse a AWS CLI comandos utilizando el --region parámetro, o establecerse como la región predeterminada para un perfil utilizando el aws configure comando. También puede definir la región al hacer llamadas mediante el SDK de AWS. Para obtener más información, consulte la documentación del SDK de su lenguaje de programación específico.

Solucionar problemas con comandos de Docker al utilizar Amazon ECR

Temas

En algunos casos, al ejecutar un comando de Docker en Amazon ECR se genera un mensaje de error. A continuación se explican algunos de los mensajes de error más comunes y sus posibles soluciones.

Error "Error de verificación de sistema de archivos" o "404: Imagen no encontrada" Al extraer una imagen de un Amazon ECR Repositorio

Puede recibir el error `Filesystem verification failed` al utilizar el docker pull comando para extraer una imagen de un Amazon ECR repositorio con Docker 1.9 o superior. Es posible que reciba el error `404: Image not found` cuando utilice versiones de Docker anteriores a la 1.9.

A continuación se explican los posibles motivos.

El disco local está lleno

> Si el disco local en el que ejecuta el comando docker pull está lleno, es posible que el hash SHA-1 que se haya calculado en el archivo local sea distinto del que haya calculado Amazon ECR. Compruebe que el disco local cuenta con suficiente espacio libre para almacenar la imagen de Docker que está extrayendo. Puede eliminar imágenes antiguas y así hacer sitio para las nuevas. Ejecute el comando docker images para ver una lista de las imágenes de Docker descargadas localmente y sus tamaños.

El cliente no se puede conectar al repositorio remoto debido a un error de red.

> Las llamadas a un repositorio de Amazon ECR requieren conexión a Internet. Verifique la configuración de red y compruebe que otras herramientas y aplicaciones sí pueden obtener acceso a recursos en Internet. Si está ejecutando docker pull en un Amazon EC2 en una subred privada, verifique que la subred tenga una ruta a Internet. Utilice un servidor de conversión de las direcciones de red (NAT) o una gateway de NAT administrada.
>
> Actualmente, las llamadas a un Amazon ECR también requiere acceso de red a través de su firewall corporativo a Amazon Simple Storage Service (Amazon S3). Si su organización utiliza un firewall o un dispositivo NAT que permite excepciones de puntos de enlace de servicio, asegúrese de que los puntos de enlace de servicio de Amazon S3 de su región actual figuren estén permitidos.
>
> Si está usando Docker tras un proxy HTTP, puede configurar Docker con los ajustes del proxy correspondientes. Para obtener más información, consulte Proxy HTTP en la documentación de Docker.

Error "Error de verificación de capa de sistema de archivos" al extraer imágenes de Amazon ECR

Puede recibir el error `image image-name not found` al tirar de imágenes con el docker pull comando. Si revisa los logs de Docker, es posible que encuentre un error como el siguiente:

```
filesystem layer verification failed for digest sha256:2b96f...
```

Este error indica que no se han podido descargar una o varias capas de la imagen. A continuación se explican los posibles motivos.

Está usando una versión antigua de Docker

Este error puede ocurrir en un reducido porcentaje de casos al utilizar una versión de Docker anterior a la 1.10. Actualice Docker a la versión 1.10 o a una posterior.

El cliente ha detectado un error de red o disco

Un disco completo o un problema de red pueden impedir que se descarguen uno o más niveles, como se discutió anteriormente sobre `Filesystem verification failed` mensaje. Siga las recomendaciones anteriores para asegurarse de que su sistema de archivos no está lleno y de que ha habilitado el acceso a Amazon S3 desde su red.

Errores HTTP 403 o error "no basic auth credentials" al enviar contenido a un repositorio

Hay ocasiones en las que puede recibir un `HTTP 403 (Forbidden)` error o el mensaje de error `no basic auth credentials` desde el docker push o docker pull comandos, incluso si se ha autenticado correctamente a Docker utilizando el aws ecr get-login-password comando. A continuación se indican algunas causas conocidas de este problema:

Se ha autenticado en una región diferente

Las solicitudes de autenticación están vinculadas con regiones específicas y no se pueden utilizar en otras regiones. Por ejemplo, si obtiene un código de autorización de EE.UU. Oeste (Oregón), no puede utilizarlo para autenticarse en sus repositorios en US East (N. Virginia). Para resolver el problema, asegúrese de haber recuperado un token de autenticación de la misma región en la que se encuentra el repositorio.

Se ha autenticado para enviar a un repositorio para el que no tiene permisos

No dispone de los permisos necesarios para enviar al repositorio. Para obtener más información, consulte Políticas de repositorio (p. 29).

Su token ha caducado.

El periodo predeterminado de vencimiento de los tokens de autorización obtenidos mediante la operación `GetAuthorizationToken` es de 12 horas.

Error en `wincred` gestor de credenciales

Algunas versiones de Docker para Windows utilizan un administrador de credenciales llamado `wincred`, que no gestiona correctamente el comando de inicio de sesión de Docker producido por aws ecr get-login (para obtener más información, consulte https://github.com/docker/docker/issues/22910). Puede ejecutar el comando de inicio de sesión de Docker generado, pero si intenta enviar o extraer imágenes, el comando falla. Puede trabajar en torno a este error quitando el `https://` esquema del argumento del registro en el comando de inicio de sesión de Docker que es salida desde aws ecr get-login. A continuación, se muestra un comando de inicio de sesión de Docker sin el esquema HTTPS.

```
docker login -u AWS -p <password> <aws_account_id>.dkr.ecr.<region>.amazonaws.com
```

Solución de problemas Amazon ECR Mensajes de error

En algunos casos, una llamada de API que ha activado a través de la Amazon ECS o la consola AWS CLI sale con un mensaje de error. A continuación se explican algunos de los mensajes de error más comunes y sus posibles soluciones.

Error "Error respuesta de Daemon: Criterio de valoración de registro no válido" cuando se inicia sesión de AWS ecr

Puede ver el siguiente error al ejecutar el aws ecr get-login comando para obtener las credenciales de inicio de sesión para su Amazon ECR repositorio:

```
Error response from daemon: invalid registry endpoint
    https://xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/v0/: unable to ping registry
 endpoint
    https://xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/v0/
v2 ping attempt failed with error: Get https://xxxxxxxxxxxx.dkr.ecr.us-
east-1.amazonaws.com/v2/:
    dial tcp: lookup xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com on 172.20.10.1:53:
    read udp 172.20.10.1:53: i/o timeout
```

Este error puede producirse en sistemas MacOS X y Windows en los que se esté ejecutando Docker Toolbox, Docker para Windows o Docker para Mac. A menudo se produce cuando otras aplicaciones alteran las rutas a través de la puerta de enlace local (192.168.0.1) a través de la cual la máquina virtual debe llamar para acceder a la Amazon ECR servicio. Si el error ocurre al utilizar Docker Toolbox, reiniciar el entorno de Docker Machine o el sistema operativo del cliente local suele resolverlo. Si esto no resuelve el problema, utilice el comando docker-machine ssh para iniciar sesión en su instancia de contenedor. Realice una búsqueda de DNS en un host externa para verificar que ve los mismos resultados que ha visto en su host local. Si los resultados son diferentes, consulte la documentación de Docker Toolbox para asegurarse de que el entorno de Docker Machine está configurado correctamente.

HTTP 429: Demasiadas solicitudes o excepción de limitación

Puede recibir un `429: Too Many Requests` error o un `ThrottleException` error de uno o más Amazon ECR comandos o llamadas API. Si utiliza herramientas de acoplador con Amazon ECR, a continuación, para las versiones 1.12.0 y superiores del acoplador, puede ver el mensaje de error `TOOMANYREQUESTS: Rate exceeded`. Para las versiones de Docker por debajo de 1.12.0, puede ver el error `Unknown: Rate exceeded`.

Esto indica que está realizando repetidamente una llamada a un único punto de enlace en Amazon ECR en poco tiempo y que se están limitando sus solicitudes. La limitación controlada ocurre cuando el número de llamadas que realiza un usuario a un único punto de enlace supera una determinada cantidad en un periodo establecido.

Las operaciones de API en Amazon ECR tienen limitaciones distintas.

Por ejemplo, el acelerador para el `GetAuthorizationToken` La acción es de 20 transacciones por segundo (TPS), con una ráfaga de hasta 200 TPS permitida. En cada región, cada cuenta recibe un cubo que puede almacenar hasta 200 `GetAuthorizationToken` créditos. Estos créditos se reaprovisionan a

la velocidad de 20 por segundo. Si su bucket tiene 200 créditos, podría realizar hasta 200 transacciones de API `GetAuthorizationToken` por segundo durante un segundo, y luego 20 transacciones por segundo de forma indefinida.

Para gestionar errores de limitación controlada, implemente una función de reintento con retardo exponencial en el código. Para obtener más información, consulte Reintentos de error y retroceso exponencial en AWS en el Referencia general de Amazon Web Services.

HTTP 403: "El usuario [arn] no está autorizado a realizar [operación]"

Es posible que aparezca el siguiente error al intentar ejecutar una acción con Amazon ECR:

```
$ aws ecr get-login
A client error (AccessDeniedException) occurred when calling the GetAuthorizationToken
 operation:
    User: arn:aws:iam::account-number:user/username is not authorized to perform:
    ecr:GetAuthorizationToken on resource: *
```

Esto indica que al usuario no se le han concedido permisos para utilizar Amazon ECR o que los permisos no están configurados correctamente. Si está realizando acciones en un repositorio de Amazon ECR, compruebe que el usuario tiene permisos de acceso a dicho repositorio. Para obtener más información sobre cómo crear y comprobar permisos para Amazon ECR, consulte Identity and Access Management para Amazon EC2 Container Registry (p. 70).

HTTP 404: "El repositorio no existe" Error

Si especifica un repositorio de Docker Hub que no existe actualmente, Docker Hub lo crea de forma automática. En Amazon ECR, es necesario crear explícitamente los nuevos repositorios para poder utilizarlos. Esto impide que se creen nuevos repositorios por accidente (por ejemplo, debido a errores ortográficos) y también permite asegurarse de que a cada nuevo repositorio se le asigne explícitamente una política de acceso de seguridad adecuada. Para obtener más información sobre la creación de repositorios, consulte Repositorios privados deAmazon ECR (p. 25).

Solución de problemas de escaneo de imágenes

A continuación se presentan errores comunes de escaneo de imágenes. Puede ver errores como este en el Amazon ECR mediante la visualización de los detalles de la imagen o a través de la API o AWS CLI utilizando el `DescribeImageScanFindings` API.

UnsupportedImageError

Puede obtener un `UnsupportedImageError` error al intentar escanear una imagen construida utilizando un sistema operativo que Amazon ECR no admite escaneo de imágenes para. Amazon ECR admite el escaneado de vulnerabilidad de paquete para las versiones principales de Amazon Linux, , Amazon Linux 2Distribuciones de Linux, Debian, Ubuntu, centos, Oracle Linux, Alpine y RHEL Linux. Una vez que una distribución pierde apoyo de su proveedor, Amazon ECR puede que ya no sea compatible con la exploración de vulnerabilidades. Amazon ECR no admite imágenes de escaneado creadas desde el Arañazos de acoplador imagen.

Un `UNDEFINED` se devuelve el nivel de gravedad

Puede recibir un hallazgo de exploración que tenga un nivel de gravedad de `UNDEFINED`. Las siguientes causas son las causas comunes de esto:

- El origen de CVE no asignó prioridad a la vulnerabilidad.
- A la vulnerabilidad se le asignó una prioridad que Amazon ECR no reconocía.

Para determinar la gravedad y la descripción de una vulnerabilidad, puede ver las CVE directamente desde el origen.

Historial de revisión

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de Amazon ECR. Actualizamos la documentación con frecuencia para dar cuenta de los comentarios que nos envía.

Cambio	Descripción	Fecha
La replicación entre regiones y cuentas	Amazon ECR ha añadido compatibilidad para configurar los ajustes de replicación del registro privado. Para obtener más información, consulte Configuración de registros privados (p. 17).	8 de diciembre de 2020
Compatibilidad con artefactos OCI	El Amazon ECR es ahora compatible con la inserción y extracción de artefactos OCI (Open Container Initiative). Se ha añadido un nuevo parámetro `artifactMediaType` a la respuesta de la API `DescribeImages` para indicar el tipo de artefacto. Para obtener más información, consulte Inserción de un gráfico de Helm (p. 41).	24 de agosto de 2020
Cifrado en reposo	El Amazon ECR de AWS Key Management Service ahora permite configurar el cifrado de los repositorios utilizando el cifrado del lado del servidor con claves maestras del cliente (CMK) almacenadas en AWS KMS (). Para obtener más información, consulte Cifrado en reposo (p. 89).	29 de julio de 2020
Imágenes multiarquitectura	Amazon ECR añadió compatibilidad para crear y empujar listas de manifiesto Docker que se utilizan para imágenes multiarquitectura. Para obtener más información, consulte Empujar una imagen multiarquitectura (p. 40).	28 de abril de 2020
Métricas de uso de Amazon ECR	Se han agregado métricas de uso de CloudWatch en Amazon ECR que proporcionan visibilidad sobre el uso de los recursos de la cuenta. Además, es posible crear alarmas de CloudWatch desde las consolas de CloudWatch yCuotas de servicio para recibir alertas cuando el uso se acerque a la cuota de servicio aplicada. Para obtener más información, consulte Métricas de uso de Amazon ECR (p. 103).	28 de febrero de 2020
Se han actualizado las cuotas de servicio de Amazon ECR	Se han actualizado las cuotas de servicio de Amazon ECR para incluir las cuotas de cada API. Para obtener más información, consulte Amazon ECRCuotas de servicio de (p. 115).	19 de febrero de 2020
Comando `get-login-password` agregado	Se ha agregado compatibilidad para get-login-password, que proporciona un método simple y seguro para recuperar un token de autorización.	4 de febrero de 2020

Cambio	Descripción	Fecha
	Para obtener más información, consulte Usar un token de autorización (p. 15).	
Escaneo de imágenes	Se ha añadido compatibilidad para el escaneo de imágenes, lo que ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. Amazon ECR utiliza la base de datos Vulnerabilidades y exposiciones comunes (CVE) del proyecto de CoreOS Clair de código abierto y le proporciona una lista de resultados de análisis. Para obtener más información, consulte Escaneo de imágenes (p. 59).	24 de octubre de 2019
Política de punto de enlace de la VPC	Se ha añadido compatibilidad para configurar una política de IAM en los puntos de enlace de la VPC de la interfaz de Amazon ECR. Para obtener más información, consulte Cree una política de criterios de valoración para su Amazon ECR Criterios de valoración VPC (p. 99).	26 de septiembre de 2019
Mutabilidad de etiquetas de imágenes	Se ha agregado compatibilidad para configurar un repositorio que sea inmutable y evitar que las etiquetas de imagen se sobrescriban. Para obtener más información, consulte Mutabilidad de etiquetas de imágenes (p. 58).	25 de julio de 2019
Puntos de enlace de la VPC de tipo interfaz (AWS PrivateLink)	Se ha agregado compatibilidad para configurar puntos de enlace de la VPC de interfaz basados en AWS PrivateLink. Esto le permite crear una conexión privada entre su VPC y Amazon ECR sin necesidad de obtener acceso a través de Internet, a través de una instancia NAT, una conexión de VPN o AWS Direct Connect. Para obtener más información, consulte Amazon ECR interfaces VPC de interfaz (AWS privatelink) (p. 95).	25 de enero de 2019
Etiquetado de recursos	Amazon ECR ha añadido compatibilidad con la adición de etiquetas de metadatos a sus repositorios. Para obtener más información, consulte Etiquetado de un repositorio deAmazon ECR (p. 35).	18 de diciembre de 2018
Cambio de nombre de Amazon ECR	Se ha cambiado el nombre de Amazon EC2 Container Registry (anteriormente se llamaba Amazon EC2 Container Registry).	21 de noviembre de 2017
Políticas de ciclo de vida	Las políticas de ciclo de vida de Amazon ECR le permiten especificar la administración de ciclo de vida de las imágenes de un repositorio. Para obtener más información, consulte Políticas de ciclo de vida (p. 47).	11 de octubre de 2017

Cambio	Descripción	Fecha
Amazon ECR admite el manifiesto de imágenes de Docker 2, esquema 2	Amazon ECR admite ahora el manifiesto de imágenes de Docker V2, esquema 2 (que se usa con Docker versión 1.10 y posteriores). Para obtener más información, consulte Formatos del manifiesto de imágenes de contenedor (p. 63).	27 de enero de 2017
Disponibilidad general de Amazon ECR	Amazon EC2 Container Registry (Amazon ECR) es un servicio de registro administrado de Docker de AWS seguro, escalable y fiable.	21 de diciembre de 2015

AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.